Safe Nuclear Power: Instrumentation, Human Oversight, and Infrastructure Transition

ECE 4900W – Summer 2025

Arturo Salinas-Aguayo

University of Connecticut
College of Engineering

June 9, 2025

Safe Nuclear Power

Safe Nuclear Power: Instrumentation, Human Oversight, and Infrastructure Transition
ECE 4900W – Summer 2025

Arturo Salinas-Aguayo

University of Connecticut
College of Engineering

June 9, 2025

Welcome. This presentation explores the technological, ethical, and infrastructural dimensions of nuclear power in the modern world. We will cover lessons from historic accidents, instrumentation, human-machine interface design, and current innovations. Each story reveals both vulnerability and resilience.

Outline

Here is the roadmap for this presentation. Each section builds on the last, culminating in a call for renewed responsibility and innovation in the nuclear field.


E=mc²

Motivation

- High energy density and steady base-load power
- Nearly zero emissions, independent of weather
- Risks of failure—catastrophic if unmanaged

Despite fears, nuclear remains one of the most efficient and clean energy sources. But it requires precision and care at every level.

The Fission Process

$$^{235}\text{U} +^{1} \text{n} \rightarrow^{92} \text{Kr} +^{141} \text{Ba} + 3^{1}\text{n} + \text{Energy} \approx 200 \text{ MeV} \quad (1)$$

- A neutron collides with uranium-235, causing it to split
- Releases energy and more neutrons $\rightarrow$ possible chain reaction

The Fission Process

$$^{235}\mathrm{U} + ^{1}\mathrm{n} \rightarrow ^{92}\mathrm{Kr} + ^{141}\mathrm{Ba} + 3^{1}\mathrm{n} + \text{Energy} \approx 200\ \text{MeV} \quad (1)$$

- A neutron collides with uranium-235, causing it to split
- Releases energy and more neutrons → possible chain reaction

This is the reaction that drives nuclear power. The energy release is immense, but so is the potential for instability if left uncontrolled.

Reactivity and Control

$$\rho = \frac{k_{\text{eff}} - 1}{k_{\text{eff}}} \tag{2}$$

- k_{eff}: effective neutron multiplication factor
- $\rho > 0$: supercritical (power increases)
- $\rho = 0$: critical (steady power)
- $\rho < 0$: subcritical (power decreases)

Instrumentation exists to measure and control reactivity—avoiding runaway reactions like those at SL-1 and Chernobyl.

Reactivity and Control

$$\rho = \frac{k_{\text{eff}} - 1}{k_{\text{eff}}} \tag{2}$$

- k_{eff}: effective neutron multiplication factor
- $\rho > 0$: supercritical (power increases)
- $\rho = 0$: critical (steady power)
- $\rho < 0$: subcritical (power decreases)

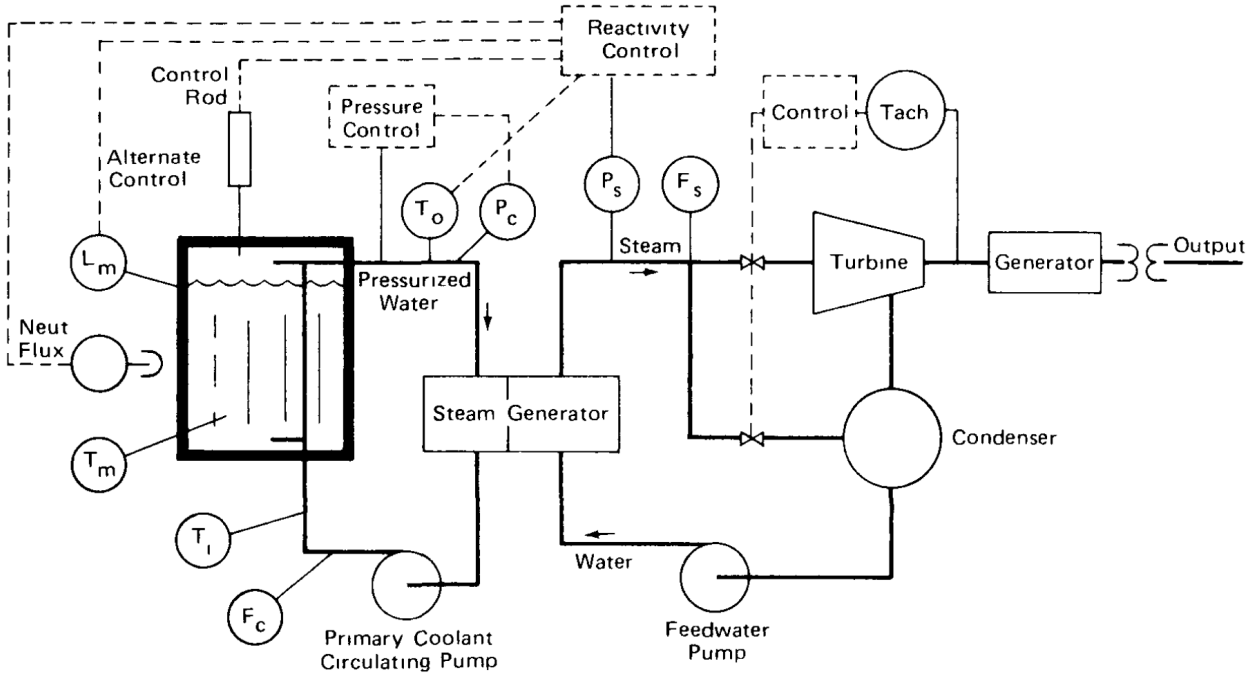
Types of Reactors

- Pressurized Water Reactor (PWR)
- Boiling Water Reactor (BWR)
- Heavy Water Reactor (CANDU)
- Advanced Gas-cooled Reactor (AGR)

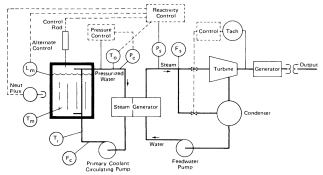
- Pressurized Water Reactor (PWR)
- Boiling Water Reactor (BWR)
- Heavy Water Reactor (CANDU)
- Advanced Gas-cooled Reactor (AGR)

Each design uses different coolants and moderators, which affect safety logic and monitoring strategies.

PWR Instrumentation



PWR Instrumentation



PWRs are the most common worldwide. Sensors track neutron flux, coolant temperature, rod position, pressure, and flow rate.

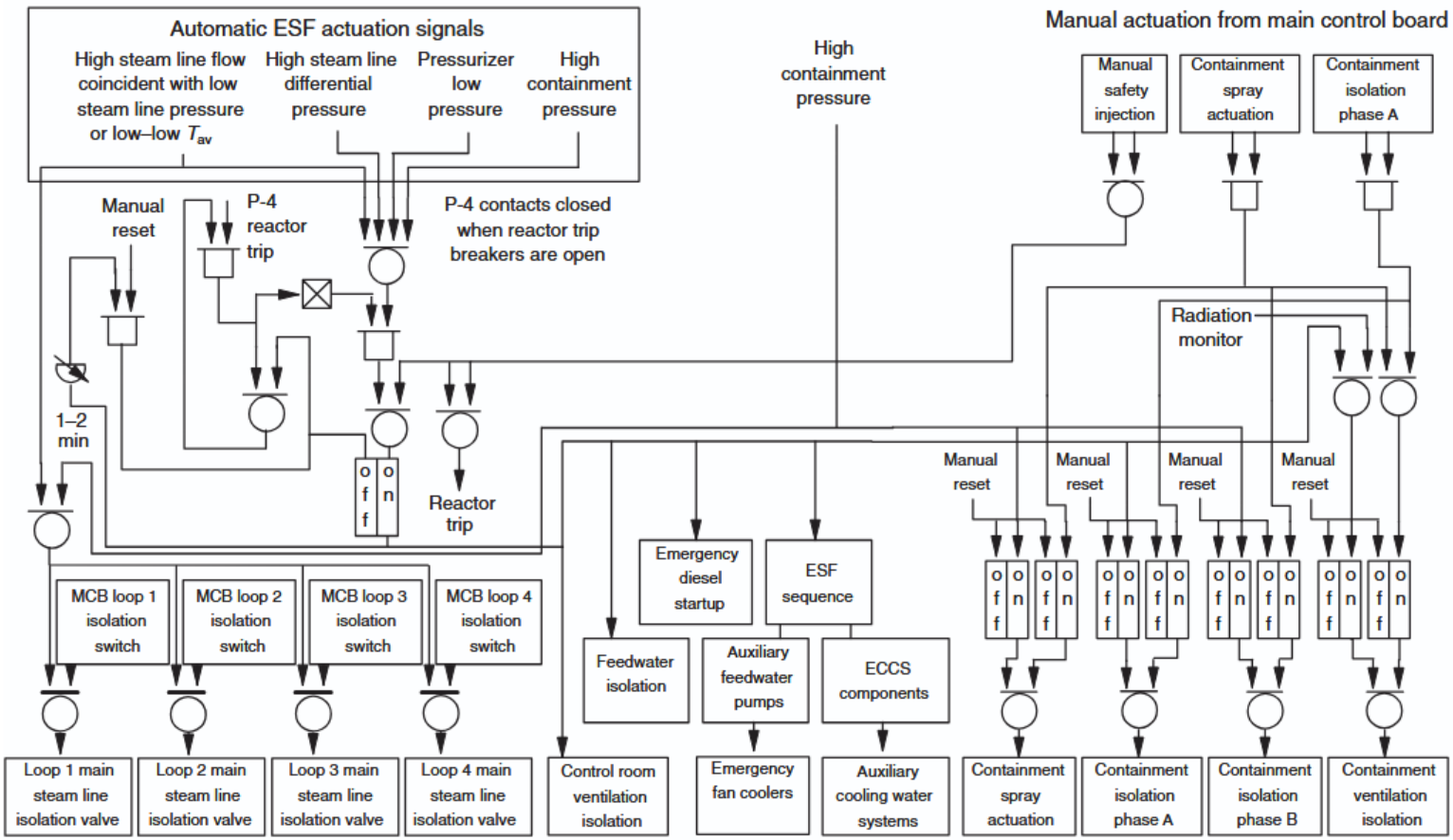
Automatic Protection Systems

- Reactor protection systems (RPS): monitor reactivity, temperature, pressure
- Logic interlocks: prevent unsafe configurations
- Hardwired paths with digital backups

- Reactor protection systems (RPS): monitor reactivity, temperature, pressure
- Logic interlocks: prevent unsafe configurations
- Hardwired paths with digital backups

Even the best operator can't always react fast enough. That's where automatic systems step in. SCRAMs instantly insert control rods. Protection logic compares real-time data to safety limits, triggering shutdowns, alarms, or backup actuation.

Control Logic



SL-1: Prompt Critical Accident

Local firefighters arrived in response to a fire alarm and found the facility abandoned. Coffee cups remained warm, and food was left uneaten. As radiation alarms activated on their dosimetry equipment, they realized a serious radiological event had occurred. Two operators were located dead from radiation exposure. The third, Richard Legg, was discovered impaled and pinned to the containment ceiling by a control rod—ejected upward during the reactor's prompt critical event.

SL-1: Prompt Critical Accident

- Occurred January 3, 1961 in Idaho Falls.
- A single control rod was withdrawn manually beyond safe limits.
- Caused an instantaneous power excursion and steam explosion.
- All three operators died; first fatal U.S. nuclear accident.

SL-1: Prompt Critical Accident

- Occurred January 3, 1961 in Idaho Falls.
- A single control rod was withdrawn manually beyond safe limits.
- Caused an instantaneous power excursion and steam explosion.
- All three operators died; first fatal U.S. nuclear accident.

Despite repeated reports of sticking rods, the system lacked mechanical or procedural interlocks to prevent rapid withdrawal. A single operator retained full manual control, with no redundancy or supervisory lockouts. The SL-1 event shows the critical role of human factors engineering, particularly in minimizing design interfaces that allow unsafe manual operations

Three Mile Island: Partial Core Meltdown

The Three Mile Island Unit 2 (TMI-2) accident occurred on March 28, 1979, near Harrisburg, Pennsylvania, and remains the most serious commercial nuclear accident in the United States. It was precipitated by the failure of a pressure-operated relief valve (PORV) that became stuck open during a minor malfunction. The valve allowed coolant to escape from the pressurizer, but due to inadequate instrumentation, operators believed it had closed properly

Three Mile Island: Partial Core Meltdown

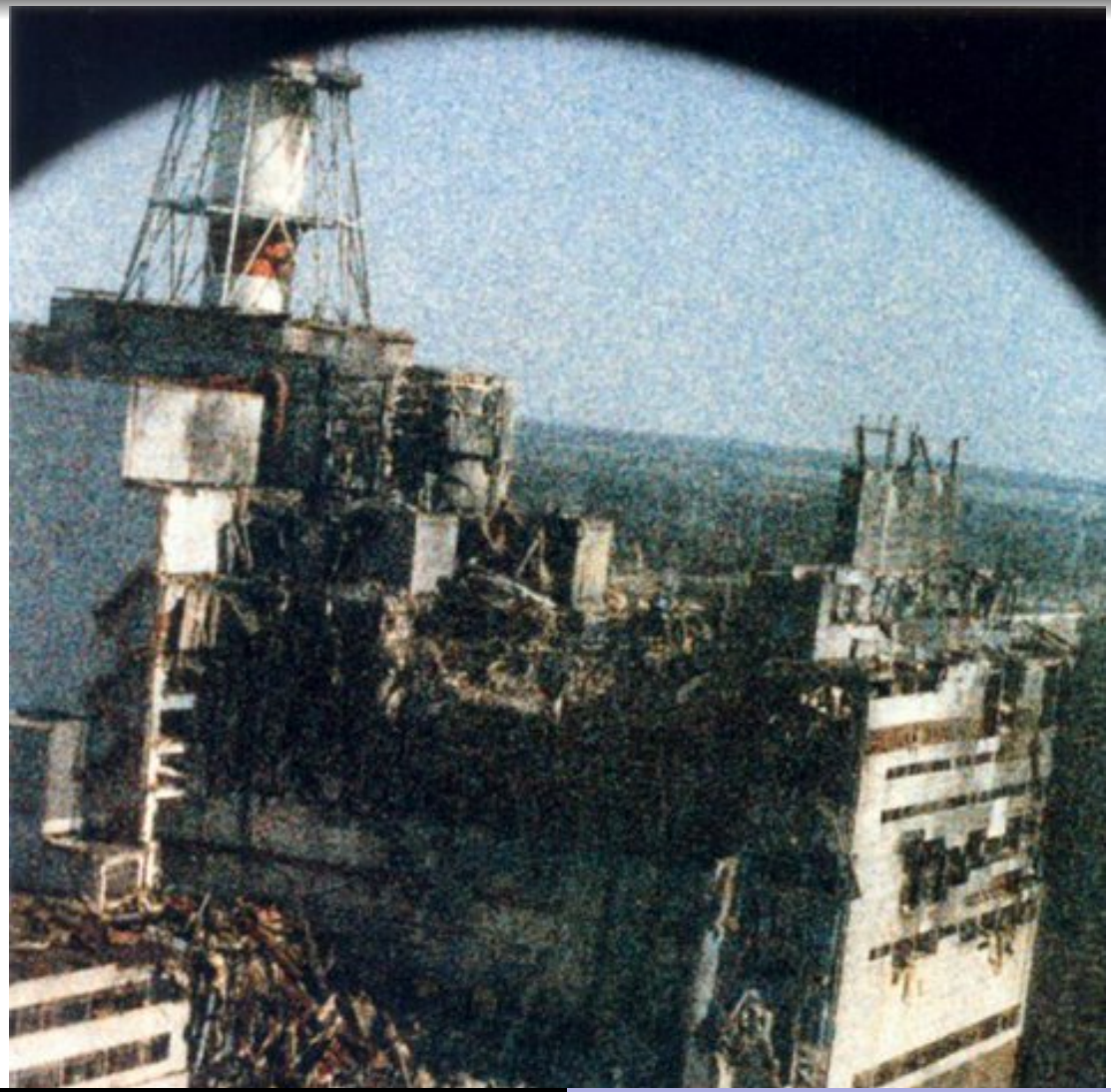
- March 28, 1979 in Pennsylvania.
- Equipment failure: relief valve stuck open.
- Operator misinterpretation led to coolant pump shutdown.
- Reactor overheated—partial meltdown of core.

Three Mile Island: Partial Core Meltdown

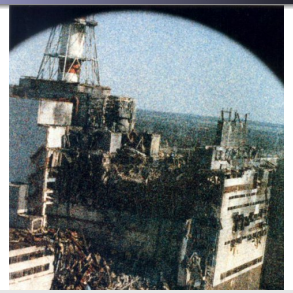
- March 28, 1979 in Pennsylvania.
- Equipment failure: relief valve stuck open.
- Operator misinterpretation led to coolant pump shutdown.
- Reactor overheated—partial meltdown of core.

Prior to this event, the relationship between human performance and system design was underappreciated in reactor control engineering. It was often assumed that proper training and "common sense" would be sufficient for managing system faults. However, the TMI- 2 accident highlighted that even well-trained operators can make catastrophic errors when systems are not designed to support human cognition under stress. As a result of this accident, the field of human factors engineering gained legitimacy within the nuclear industry. Organizational and industrial psychology—especially the study of ergonomics and operator-centered design—emerged as crucial disciplines in instrumentation and control system development [6]. Operators needed interfaces not merely for function, but for situational awareness and decision-making under pressure. This marked a turning point in control room design philosophies, ushering in era-defining updates to alarm management, display hierarchy, and interface logic

Chernobyl: Uncontrolled Power Surge



Chernobyl: Uncontrolled Power Surge



The test intended to verify whether the rotational inertia of the turbine could temporarily power the emergency coolant pumps in the event of a grid power failure [7]. The RBMK-1000 reactor involved was a Soviet-designed graphite- moderated, water-cooled system—flawed by both design and execution

Chernobyl: Uncontrolled Power Surge

- April 26, 1986 in Pripyat, USSR.
- Unsafe test conducted at low power with flawed RBMK reactor.
- Positive void coefficient caused rapid reactivity increase.
- Control rods exacerbated the surge due to graphite tips.
- Reactor exploded; massive radioactive release.

Chernobyl: Uncontrolled Power Surge

- April 26, 1986 in Pripyat, USSR.
- Unsafe test conducted at low power with flawed RBMK reactor.
- Positive void coefficient caused rapid reactivity increase.
- Control rods exacerbated the surge due to graphite tips.
- Reactor exploded; massive radioactive release.

The core overheated instantly, rupturing fuel channels and vaporizing coolant. A vi- olent steam explosion lifted the reactor's 2,000-ton upper biological shield. A second ex- plosion—possibly from hydrogen or steam—further breached the structure and exposed the graphite moderator, which caught fire. Figure 6 shows the aftermath of the explosion mere hours after the explosion. The fire lofted radioactive particles into the upper atmosphere, affecting much of Europe

The aftermath of Chernobyl catalyzed global reevaluation of nuclear safety, reactor de- sign, and operator training. The international community pushed for increased transparency, safety audits, and enhanced containment strategies. The photograph in Figure 7 famously shows the "Elephant's Foot," a deadly corium formation. The strange visual static in the image is not lightning, but film degradation from intense radiation—testament to the un- precedented radioactive environment at the site

Fukushima Daiichi: Station Blackout

- March 11, 2011 in Japan.
- Magnitude 9.0 earthquake triggered tsunami.
- Backup diesel generators flooded—loss of core cooling.
- Hydrogen buildup led to explosions in three reactors.

Fukushima Daiichi: Station Blackout

- March 11, 2011 in Japan.
- Magnitude 9.0 earthquake triggered tsunami.
- Backup diesel generators flooded—loss of core cooling.
- Hydrogen buildup led to explosions in three reactors.

The Fukushima-Daiichi Nuclear Power Station, operated by TEPCO, was critically affected. Although the three operating reactors—Units 1, 2, and 3—successfully SCRAMed (shut down automatically), the tsunami flooded the site and disabled both the offsite grid connections and emergency diesel generators [12]. This unprecedented loss of power across all units is illustrated in Figure 8, which shows the reactor buildings after successive hydrogen explosions.

Operators at Fukushima recognized the danger but were rendered effectively blind by the loss of power. Unlike U.S. Navy reactor systems—where portable test equipment such as Fluke digital multimeters can be attached to terminals for passive thermocouple read- ings—the Fukushima design lacked redundant manual monitoring options. In a desperate act of ingenuity, personnel retrieved car batteries from nearby vehicles and wired them in series to restore minimal voltage to power essential instrumentation. Unfortunately, by the time this improvised power source was implemented, core damage in Units 1, 2, and 3 was already underway, with partial or full meltdown confirmed in post-event analyses

Human Operators: Essential Links

Human Operators: Essential Links

- Human error was central to SL-1, TMI, and Chernobyl.
- Operators are responsible for interpreting ambiguous or conflicting signals.
- Training, vigilance, and mental workload matter.

Human Operators: Essential Links

- Human error was central to SL-1, TMI, and Chernobyl.
- Operators are responsible for interpreting ambiguous or conflicting signals.
- Training, vigilance, and mental workload matter.

Despite automation, human judgment determines plant safety. Accidents often trace back to either misinterpretation or improper training.

Human Factors Engineering

- Post-TMI, HFE became a formal discipline in nuclear plant design.
- Goals: reduce confusion, prevent overload, clarify alarms.
- INPO and NRC led redesigns of control interfaces.

- Post-TMI, HFE became a formal discipline in nuclear plant design.
- Goals: reduce confusion, prevent overload, clarify alarms.
- INPO and NRC led redesigns of control interfaces.

Human-machine interface redesign became essential after TMI. Alarm logic, indicator layout, and system feedback were all reengineered.

Operator Training

Operator Training

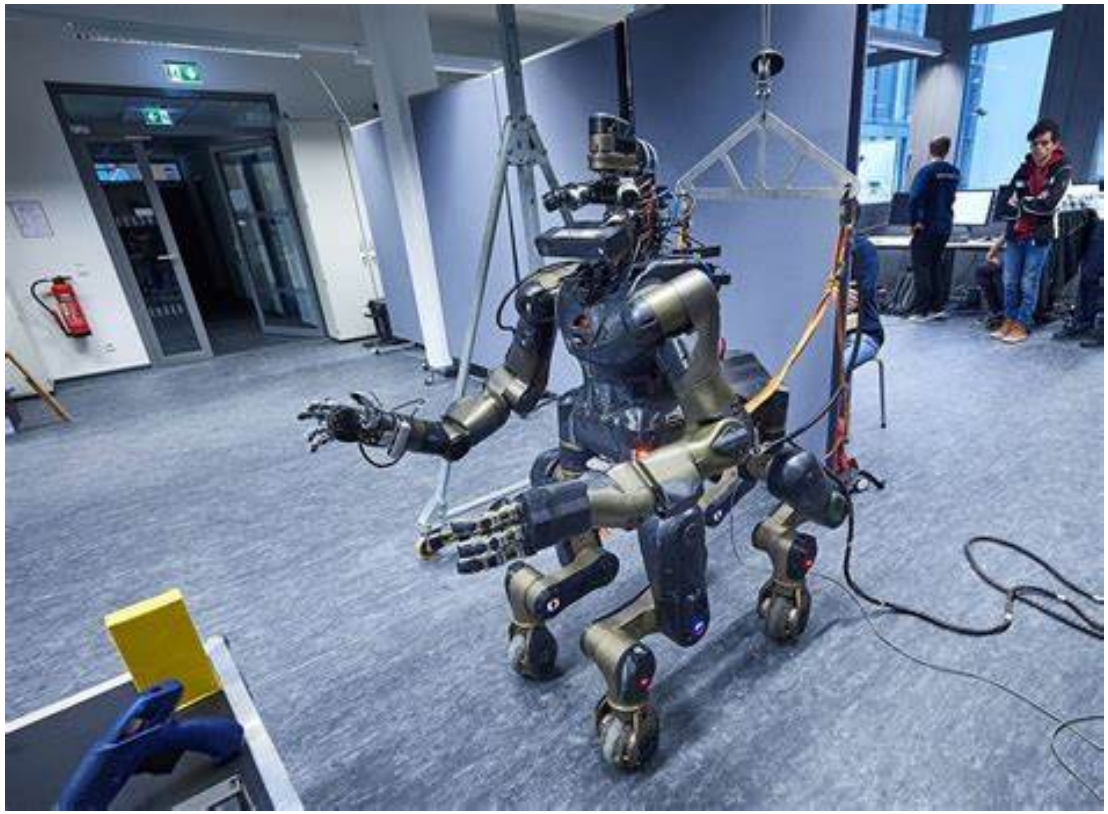
- U.S. Navy trains operators with year-long theoretical and practical curriculum.
- Qualification cards enforce step-by-step system mastery.
- Real-time simulators mimic full plant behavior—including failures.

Operator Training

- U.S. Navy trains operators with year-long theoretical and practical curriculum.
- Qualification cards enforce step-by-step system mastery.
- Real-time simulators mimic full plant behavior—including failures.

Simulators allow safe repetition of emergency scenarios. This procedural rigor is unmatched in civilian sectors.

Ethical Oversight in Automation



Ethical Oversight in Automation

- Systems must support—not replace—human oversight.
- Overreliance on automation can erode accountability.
- Ethical design considers failure modes, transparency, and operator input.

Ethical Oversight in Automation

- Systems must support—not replace—human oversight.
- Overreliance on automation can erode accountability.
- Ethical design considers failure modes, transparency, and operator input.

Designing for ethical oversight means respecting human limits while reinforcing responsibility. The worst outcomes often arise when operators are sidelined.

Why Nuclear Declined

- Each accident—from SL-1 to Fukushima—prompted strict new regulations.
- Longer licensing cycles delayed new builds by decades.
- Public opposition and fear, not technical failure, stalled the industry.
- Skilled labor and supply chains diminished as construction halted.

Why Nuclear Declined

- Each accident—from SL-1 to Fukushima—prompted strict new regulations.
- Longer licensing cycles delayed new builds by decades.
- Public opposition and fear, not technical failure, stalled the industry.
- Skilled labor and supply chains diminished as construction halted.

The world walked away not because nuclear failed—but because faith in its management eroded. Regulation became slower, and expertise drifted away.

Challenges Today

- Most operating reactors in the U.S. are past mid-life.
- Replacing the aging nuclear workforce is a growing challenge.
- Engineering firms that once supported nuclear have pivoted to renewables.
- Safety margins remain—but the supporting infrastructure has weakened.

Challenges Today

- Most operating reactors in the U.S. are past mid-life.
- Replacing the aging nuclear workforce is a growing challenge.
- Engineering firms that once supported nuclear have pivoted to renewables.
- Safety margins remain—but the supporting infrastructure has weakened.

Many of the companies and capabilities that built the first generation of plants no longer exist in their original form.

Conclusion: A Deliberate Future

Conclusion: A Deliberate Future

- Nuclear safety is engineered, not assumed.
- Instrumentation and human oversight must evolve together.
- Ethical design puts operators in control, not out of the loop.
- The tools are available—what remains is the will to rebuild trust.

Conclusion: A Deliberate Future

- Nuclear safety is engineered, not assumed.
- Instrumentation and human oversight must evolve together.
- Ethical design puts operators in control, not out of the loop.
- The tools are available—what remains is the will to rebuild trust.

Safe nuclear power isn't an inevitability—it's a discipline. What matters is not just how reactors are built, but how they are overseen.