



*An Online CPD Course
brought to you by
CEDengineering.ca*

Ethical Use Of Agentic And Generative AI In Engineering

Course No: LE2-027

Credit: 2 PDH

Brian Lisiewski, P.E.



Continuing Education and Development, Inc.

P: (877) 322-5800

info@cedengineering.ca

Table of Contents

Module 1: Introduction — AI in Engineering and the Need for Ethical Practice.....	1
1.1 Why Focus on Ethics in AI for Engineers?.....	2
Module 2: Understanding Generative and Agentic AI.....	3
Module 3: Ethical Foundations — Professional Responsibilities in the Age of AI.....	6
Module 4: AI Applications and Ethical Considerations Across Engineering Disciplines... 	9
4.1 Civil & Structural Engineering.....	9
4.2 Mechanical & Aerospace Engineering	11
4.3 Electrical & Computer Engineering	13
4.4 Chemical & Biomedical Engineering.....	15
4.5 Software & Systems Engineering.....	17
4.6 Environmental Engineering	20
Module 5: Ensuring Ethical Use of AI — Guidelines and Best Practices	22
Module 6: Summary and Conclusion	25
References	27

Module 1: Introduction — AI in Engineering and the Need for Ethical Practice

This course focuses on the ethical use of agentic and generative artificial intelligence (AI) in engineering practice. Modern engineering is experiencing a rapid integration of artificial intelligence technologies. Artificial intelligence is no longer just a concept for the future—it's now extensively applied in **engineering design, analysis, and project management**. Engineers use **machine learning models** for tasks like predicting infrastructure loads or identifying potential mechanical failures. They utilize **generative design software** to develop optimized parts, implement **smart sensors and control systems** for automated monitoring of structures and processes, and depend on **AI-powered decision-support tools** across various fields such as civil engineering and chemical processing. Two particularly transformative classes of AI have emerged in recent years:

- **Generative AI** – AI systems that create new content or designs based on patterns learned from data. Examples include large language models that generate human-like text, algorithms that produce **design alternatives** for mechanical parts or building structures, and image-generation tools that render conceptual drawings. Generative AI can rapidly produce design schematics, technical reports, simulations, or even code, serving as a creative assistant in engineering tasks.
- **Agentic AI** – AI “agents” that not only generate outputs but also **autonomously act upon them**. These systems use AI to make decisions or perform tasks with minimal human intervention. For instance, an AI agent might analyze data from a network of sensors and automatically adjust control settings in a chemical plant, or coordinate a fleet of autonomous construction robots to optimize a project schedule. In short, generative AI produces content, whereas agentic AI uses that content to act independently. Agentic AI leverages generative models for tasks like planning actions, enabling complex workflows but also introducing new challenges.

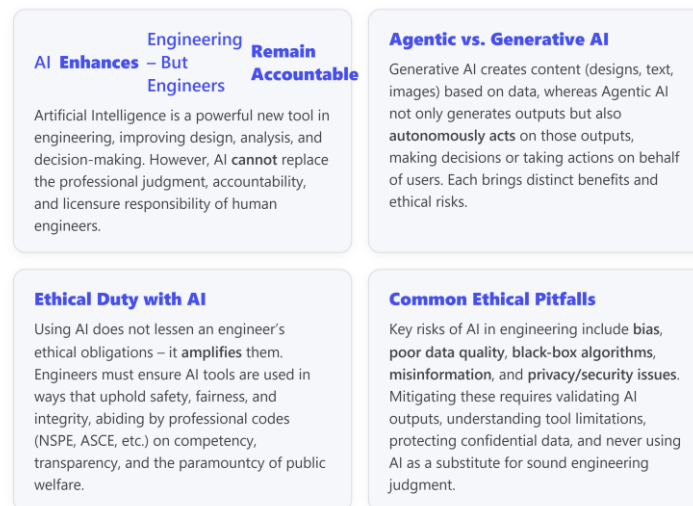


Figure 1. Key points on AI in engineering: accountability, agentic versus generative AI, ethical duty, and common pitfalls.

1.1 Why Focus on Ethics in AI for Engineers?

Engineering is governed by ethical codes and professional standards to protect the public and build trust. The NCEES Model Rules and codes like those of NSPE and ASCE require engineers to prioritize public safety, work within their expertise, and act truthfully and objectively. With AI's emergence, these responsibilities are even more crucial.

AI technologies can improve engineering efficiency and creativity but pose ethical risks if misapplied. Bias in training data may cause discrimination, black-box models hinder transparency, and unchecked AI designs risk errors. Autonomous systems can behave unpredictably, while easy content generation raises concerns about intellectual property and plagiarism. These challenges are directly tied to engineers' ethical and legal duties for competency and transparency.

Professional Competency and Lifelong Learning: The NCEES Continuing Professional Competency (CPC) standards emphasize that ongoing learning—particularly in fast-evolving fields like AI—is essential to maintain professional competence and protect the public [5]. This course addresses that need by equipping engineers with knowledge to use AI tools ethically and effectively. By understanding both the capabilities **and** limitations of AI, engineers can fulfill the directive of codes such as ASCE's Canon 1.h, which instructs engineers to “*consider the capabilities, limitations, and implications of current and emerging technologies*” as part of their work [2]. Embracing new technology offers great opportunities, but ethical practice demands caution, informed oversight, and a commitment to not let technology outpace our capacity to use it responsibly [2, 6].

In the sections that follow, we will explore how generative and agentic AI are being applied in various engineering disciplines, and what specific ethical issues and best practices arise in each context. We'll then outline general guidelines for **ethical AI integration** in engineering, grounded in professional codes and real-world lessons. Finally, a short quiz will help reinforce key concepts. As you progress, remember that **AI is a tool, not a substitute for professional engineering judgment** [1]. The licensed engineer retains ultimate responsibility for the work and must ensure that AI-assisted outputs meet the same standards of safety, quality, and compliance as any other engineering work product.

Module 2: Understanding Generative and Agentic AI

Before diving into use cases, it's important to clearly understand what we mean by **generative** and **agentic** AI, and why these categories matter for engineers.

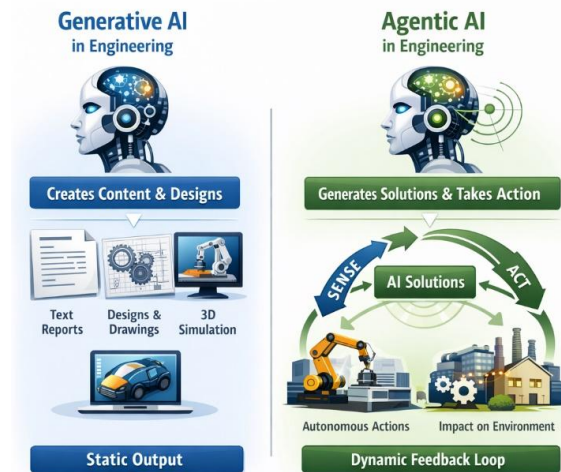


Figure 2. Generative AI creates content and designs, while agentic AI generates solutions and takes action.

- **Generative AI:** *Generative AI refers to algorithms (often based on machine learning, especially deep learning) that can produce novel content. They “generate” new data similar to the data they were trained on. Common examples include **Large Language Models (LLMs)** like ChatGPT, which generate human-like text, and image generation models that create design visuals or graphics. In engineering, generative AI can be used for tasks such as drafting technical reports, creating design prototypes or variations (e.g., generative architectural design or mechanical component shapes), suggesting code, or simulating scenarios. The output of generative AI is typically an artifact – a document, a design, a prediction, or an image. Engineers can use these outputs as **drafts or suggestions** to accelerate their work.*
 - *Example:* An engineer might use a generative AI tool to produce a first draft of a project report or to generate multiple design alternatives for a bridge truss structure based on specified parameters. The AI quickly provides several feasible designs or a well-structured text, which the engineer can then review and refine.
 - **Agentic AI:** *Agentic AI refers to AI systems (often called **AI agents**) that can make autonomous decisions or take actions to achieve goals, often interacting with their environment or software tools without needing step-by-step human guidance. These agents build upon AI’s ability to generate content by adding a level of **autonomy** – they can plan and execute tasks. Examples include **autonomous drones** or robots that navigate and perform tasks on a job site, control*

algorithms that automatically adjust engineering systems (like a smart grid management system balancing electricity distribution in real-time), or complex software agents that perform multi-step operations (for example, analyzing data and then automatically ordering maintenance or adjusting parameters in a chemical process). In short, **if generative AI produces the plan or content, agentic AI carries it out** [4].

- *Example:* A structural engineering firm might deploy an AI-based monitoring system on a bridge. This agentic AI continuously reads sensor data (strain gauges, accelerometers), detects anomalies or signs of stress, and then autonomously triggers actions – such as adjusting traffic signals to reduce load or sending an immediate alert to engineers if safety thresholds are exceeded. The system thus not only **analyzes data** (a traditional AI task) but also **takes action** by controlling external systems, exemplifying agentic behavior.



Figure 3. An engineer supervising an AI-guided robotic system on a production line.

Ethical Significance of the Distinction: Both types of AI present overlapping ethical issues (such as ensuring accuracy, avoiding bias, and maintaining accountability), but agentic AI, due to its autonomy, can **amplify risks** associated with AI use [4]. When an AI agent is not just recommending but also **implementing decisions**, errors or biases can directly translate into real-world consequences **without an immediate human in the loop**. For example, a mistake in a generative design (say, a miscalculation in a stress analysis report) is problematic, but if an engineer reviews it, they have an opportunity to catch and correct it. In contrast, an error by an autonomous agent controlling machinery could cause an accident before human intervention. As IBM’s AI ethics experts note, giving AI agents more freedom to act “**has the potential to magnify their risks,**” since less human oversight can lead to serious unintended actions [4].

Therefore, understanding whether an AI system is merely generating suggestions or actually taking autonomous actions is critical for determining the level of **scrutiny, control, and fail-safes** an engineer must implement. In both cases, the engineer must apply rigorous ethical principles, but for agentic AI the controls and accountability measures may need to be even more stringent.

Module 3: Ethical Foundations — Professional Responsibilities in the Age of AI

Engineering ethics form the bedrock of all professional practice, AI included. All **licensed engineers** are bound by codes of ethics (such as the NSPE, ASCE, IEEE, and discipline-specific codes) and state laws that enforce standards of professionalism, safety, and integrity. When incorporating AI tools into engineering work, these fundamental ethical **canons** still apply and, in some aspects, require heightened attention.

Some of the most relevant ethical **principles (Canons)** and how they relate to AI use include:

- **Paramountcy of Public Safety:** The prime directive in virtually all engineering codes (e.g., NSPE Fundamental Canon #1) is that “*Engineers shall hold paramount the safety, health, and welfare of the public.*” This means that no matter how enticing an AI-driven result is – maybe it optimizes cost or saves time – it **cannot be used if it jeopardizes public safety or wellbeing**. For instance, if a generative AI proposes a novel structural design or a transportation engineering plan, the engineer must verify that it meets all safety standards and industry codes. AI does not relieve the human engineer from the obligation to ensure designs and decisions are safe and compliant. Misuse of AI or **overreliance on unvetted AI outputs can lead to decisions that threaten public safety**, violating this foremost canon [6].
- **Competence and Technical Responsibility:** Engineers must perform services only in their **areas of competence** and must not seal or approve work not under their direct control (NSPE Canons I.2 and II.2.b) [1]. Applying this to AI: an engineer should not use an AI tool in a way that ventures beyond the engineer’s understanding of the underlying technical domain. **The engineer must have sufficient knowledge of how the AI tool works, its limitations, and the subject matter at hand to judge the tool’s output**. For example, a civil engineer using an AI to design an electrical system would be stepping outside their area of expertise, just as it would be unethical to do so without AI. Similarly, if an AI tool produces part of an engineering design or analysis, the engineer of record must ensure that the work was either created by them or under their *responsible charge* and thoroughly reviewed [1]. An engineer cannot abdicate responsibility to an AI; signing off on calculations or drawings generated by AI without proper verification and understanding is an ethical violation of the duty to act competently.
- **Truthfulness and Avoiding Deception:** Engineers must be truthful in reports, statements, and advertising and avoid deceptive acts (NSPE Fundamental Canon #5 and Code III.3) [1]. When using AI, this means being honest about the results and limitations of AI-generated work. Engineers should not present AI outputs as if they were 100% reliable or solely their own work if significant portions were generated by an AI without acknowledgment. For example, presenting a computer-generated simulation as definitive proof of safety, without clarifying its assumptions and uncertainties, could mislead clients or the public – potentially a deceptive act. **Honesty also entails acknowledging the use of AI when it materially contributes to a deliverable**. There is growing sentiment that transparency with clients or stakeholders about AI involvement is a best practice, even if not yet

legally required [1]. It fosters trust and avoids misrepresentation in cases where, say, a report or design was heavily assisted by generative AI.

- **Confidentiality and Data Privacy:** Engineers often handle sensitive client and project data. Codes of ethics (e.g., NSPE Code II.1.c) prohibit disclosing confidential information without consent [1]. Using cloud-based AI tools and services raises a critical ethical concern: **feeding proprietary or sensitive project data into an external AI system** could inadvertently violate client confidentiality if the data isn't properly protected. For instance, uploading a client's project specifications or data into a publicly available generative AI tool might expose that data to the tool's developers or risk it being included in the AI's future outputs for other users. Engineers must ensure they have permission and that proper agreements (such as non-disclosure or data handling terms) are in place before using client data in any AI service. If such guarantees can't be confirmed, it may be unethical – or even illegal – to use the AI tool with that data [1].
- **Credit and Intellectual Property:** Engineers are expected to give credit where it's due (NSPE Code III.9) and respect intellectual property rights. If an AI system draws on proprietary data or copyrighted material to produce an output, using that output could raise IP concerns. Ethically, an engineer should cite authoritative sources that an AI used, just as they would human collaborators or reference materials, especially in published reports. Additionally, claiming sole credit for work that was substantially aided by generative AI might be seen as misrepresentation. While AI itself isn't a "person" to credit, acknowledging its use (for example, noting "This design was generated using AI software and then verified by the engineering team") can demonstrate transparency and integrity [1].
- **Informed Consent and Communication:** While not always explicitly stated in codes, an emerging ethical expectation is that stakeholders should be informed when AI is used. Part of ethical practice is managing expectations and ensuring that clients or the public are not misled about how an engineering solution was derived. For example, if a city is implementing an AI-driven traffic management system (an agentic AI application in civil engineering), informing the public about how it works and what oversight is in place can aid in maintaining public trust. Clear communication about the role of AI, its benefits, and its limitations is in line with the ethical commitment to transparency and fostering trust.

Engineering Licensure and "Responsible Charge": An important concept in engineering professionalism is that of being in **responsible charge** of engineering work. Licensing laws require that a professional engineer who signs and seals a plan or report must be in responsible charge, meaning they provide **direct control and personal supervision** of the work's preparation. Using AI does not change this requirement. The NSPE has emphasized that *reviewing or accepting an AI's output without being involved in the process does not meet the responsible charge requirement* [1]. In other words, you can't simply have an AI generate a design and then sign off on it if you didn't oversee how it was done. The engineer must exercise judgment in guiding the AI, checking its work, and validating results as if a junior engineer or technician had done the work. This includes setting the parameters for generative design, verifying calculations, and testing the outputs under various scenarios. The engineer's role is to ensure that **all AI-assisted work complies with the same standards** of safety, code compliance, and quality that would apply if done manually.

By adhering to these ethical foundations when using AI, engineers help ensure that technology serves the public good without eroding trust. As we explore specific use cases in various disciplines, these core principles – safety, competence, honesty, confidentiality, and accountability – will repeatedly emerge as touchstones for ethical decision-making.

Module 4: AI Applications and Ethical Considerations Across Engineering Disciplines

AI's impact is being felt across virtually every engineering field. In this section, we highlight common AI use cases in several major engineering disciplines and discuss the unique ethical considerations and potential pitfalls in each. We will see that despite differences in applications, certain **universal ethical themes** – such as the need for validation, oversight, and alignment with human expertise – are present in all disciplines.

4.1 Civil & Structural Engineering

AI Applications: Civil engineers use AI for **predictive modeling**, **structural design optimization**, **construction management**, and infrastructure monitoring. For example, **machine learning** models can predict structural loads, traffic patterns, or maintenance needs for bridges and roads. **Generative design** algorithms propose innovative layouts for bridges, trusses, or urban plans by optimizing for factors like weight, cost, and material use. **Agentic AI** systems are emerging in construction project management – e.g., AI-driven scheduling tools that autonomously adjust project timelines or dispatch resources – and in infrastructure operation, such as intelligent traffic control systems that react in real time to congestion or autonomous inspection drones that identify structural defects in hard-to-reach places.

Ethical Issues & Best Practices: In civil engineering, the stakes are high because projects directly affect public safety on a large scale. Key ethical considerations include:

- **Safety and Reliability of AI-Generated Designs:** Any AI-generated structural design or recommendation **must be thoroughly vetted by a qualified engineer**. Civil structures (buildings, bridges, dams, etc.) must comply with building codes and safety factors. If a generative design algorithm suggests a novel bridge design, the engineer has an ethical duty to verify its structural integrity through accepted engineering principles and simulations. The recent ASCE Policy Statement 573 (2024) underscores that *AI can assist but cannot replace the training, experience, and judgment of a professional engineer in designing and operating civil projects to protect public safety* [2]. In practice, this means **never rubber-stamping an AI design without independent calculation and review**. AI might propose a thinner beam or novel geometry that appears efficient; the engineer must confirm it meets code requirements and won't jeopardize safety in worst-case conditions.
- **Transparency and Explainability:** Civil engineers often must explain and justify their designs to clients, regulators, or the public (e.g., during permitting or public consultation). Using **black-box AI models** that lack explainability can be problematic. If an AI model predicts, say, the failure risk of a dam or recommends a particular traffic pattern, the engineer should be able to explain the basis of those recommendations. The Society of Petroleum Engineers (SPE) – whose concerns parallel those in civil engineering – has highlighted that opaque AI undermines confidence because it's *“impossible to justify results to clients, regulators, or the public”* [3]. Engineers should favor interpretable models or be prepared to translate AI outputs into understandable reasoning. This might involve using **Explainable AI (XAI)** techniques or simply applying engineering fundamentals to validate AI's conclusions.

- **Data Quality and Bias in Urban Planning:** Civil engineers increasingly use AI for urban planning and infrastructure management, which may involve socioeconomic data (traffic flows, demographic information, etc.). Ethically, engineers must ensure these AIs do not propagate bias or lead to unfair outcomes for communities. For example, an AI that recommends locations for new infrastructure (like highways or facilities) might inadvertently favor certain communities and disadvantage others if trained on biased historical data. The engineer's role is to scrutinize the data and results for fairness and equity. As a cautionary tale, consider that IBM's Watson for Oncology – albeit in healthcare – produced flawed recommendations partly due to being trained on **limited, non-representative data**, illustrating how incomplete data can yield unreliable or even unsafe conclusions [3]. In civil engineering, using incomplete or regionally biased data (e.g., only one city's traffic patterns) could lead to designs that don't generalize well, causing failures or inequitable service elsewhere.
- **Automation in Construction and Operation:** Autonomous or semi-autonomous construction equipment and drones (an example of agentic AI in civil engineering) can improve efficiency and safety by handling dangerous tasks or monitoring sites. However, engineers deploying such technology must address new liabilities: if an autonomous construction machine makes a wrong decision that causes an accident, **who is responsible?** Ethically and legally, the engineer overseeing the project may hold responsibility if it was their role to ensure safe operation of tools. Proper **risk assessments, redundancies, and human override capabilities** are crucial. For instance, a self-driving earthmover should have safeguards (like emergency shutoff and geofencing) and be monitored by a human operator, especially in early implementation. The **amplified risk of agentic AI** means that without human-in-the-loop oversight, errors can have immediate physical consequences [4]. Thus, maintaining a "*human in the loop*" – someone continuously supervising and ready to intervene – is an ethical must during deployment of AI in construction or infrastructure systems.
- **Case Example – Generative Design for a Bridge:** Imagine a city engineer uses a generative AI tool to propose dozens of bridge designs for a new pedestrian bridge, aiming to minimize material use while maintaining strength. The AI produces some unconventional truss geometries that pass an initial automated stress test. Ethically, the engineer should: 1) thoroughly verify the chosen design against all relevant loads (dead, live, wind, seismic) using trusted engineering methods; 2) ensure compliance with local building codes; 3) check the AI's calculations for errors or omissions; and 4) possibly subject the design to peer review or a more transparent analysis. If the AI's design cannot be fully explained or validated, the engineer should not proceed to construction based solely on that design. This scenario underscores that **the engineer remains the final authority on safety**, not the AI.



Figure 4. A structural engineer checking an AI-proposed bridge design against calculations and building codes.

4.2 Mechanical & Aerospace Engineering

AI Applications: Mechanical engineers leverage AI for **design optimization**, **predictive maintenance**, **robotics**, and complex simulations. **Generative design** is particularly prominent in mechanical/aerospace engineering – for example, AI algorithms can automatically generate dozens of design variations for a lightweight aircraft component or an automobile part, optimizing for weight, strength, and manufacturability. These designs might have organic, non-intuitive shapes that a human designer might not have conceived on their own. In manufacturing, **robotic systems** and CNC machines increasingly use AI vision and control (an agentic form of AI) to adapt on the fly for quality control, assembly, and supply chain optimization. **Predictive maintenance** models analyze sensor data from engines, turbines, or manufacturing equipment to predict failures before they occur, allowing proactive repairs. Aerospace engineers use AI for autonomous flight control systems and trajectory optimization, as well as for analyzing big data from simulations and wind tunnel tests to improve designs.

Ethical Issues & Best Practices: Mechanical and aerospace engineering often involve safety-critical designs (vehicles, machinery, aircraft) and expensive, complex systems. Ethical use of AI in these fields emphasizes:

- **Maintaining Engineering Judgment in Design Automation:** Generative design tools can produce highly efficient shapes (for instance, an AI might design an aircraft wing rib with a complex lattice structure that reduces weight by 20%). While enticing, engineers must apply their **judgment to evaluate these AI-generated designs**. Is the design manufacturable with available materials and processes? Does it account for variability in material properties and fatigue over time? The ethical risk is that an engineer might be tempted to trust the AI's optimization blindly, given its complexity. However, professional standards (like **ASME codes** for mechanical systems or **FAA regulations** for aircraft components) require solid evidence of safety. The engineer should use traditional analysis or physical testing to validate that the design meets all requirements. If the AI's design cannot be fully

understood or tested, relying on it would be unethical. As the NSPE’s Board of Ethical Review has noted in an analogous context: technology is valuable in engineering, *“but it must never be a substitute for engineering judgment.”* Using an AI beyond the engineer’s ability to comprehend its outputs **“has a propensity to be utilized as a crutch or substitute for judgment” leading to potential liability** [1].

- System Failure and Liability in Autonomous Systems:** In both manufacturing and aerospace, agentic AI often takes the form of **autonomous or semi-autonomous systems** (e.g., self-driving vehicles, pilot-assist systems in aircraft, or intelligent industrial robots on a factory floor). These systems can pose immediate physical dangers if they malfunction. Engineers integrating such technologies must consider fail-safe designs. Ethically, it is imperative to build in **redundancies and manual override** options. For example, an autonomous delivery drone (aerospace engineering) should have collision-avoidance AI, but the engineers should still implement an override mechanism for a human controller to take over if the AI behaves unexpectedly. The question of liability is crucial: if an AI agent makes a decision that results in an accident (say, a robotic arm on an assembly line injures a worker or an autonomous drone crashes), the responsible professional engineers and their organizations will likely be held accountable for not ensuring adequate safety measures. Therefore, deploying agentic AI requires rigorous testing under a wide range of scenarios (including “edge cases”), adherence to industry safety standards, and often incremental introduction (e.g., using AI in an assistive role before granting full autonomy). As one IBM expert noted, when agentic AI can execute actions like running code or controlling machines, *“so many things could go wrong”* without proper safeguards [4] – a reminder that **engineers must proactively anticipate and mitigate failure modes** of autonomous AI systems.



Figure 5. Generative design of a lattice bracket, followed by the engineer’s stress analysis and final validation.

- Predictive Maintenance and Data Integrity:** Predictive maintenance AI models in mechanical systems (like those monitoring jet engines or factory equipment) can help prevent accidents by warning of part failures. However, if these models are based on data-driven learning, their accuracy and bias need scrutiny. An ethical engineer must ask: Is the sensor data reliable and free of tampering? Does the model account for all operating conditions or could it give false negatives/positives? Blind

trust in a maintenance AI could lead to either unnecessary part replacements (inconvenience and cost) or, worse, missing a critical failure warning. **Always have human review of AI-generated maintenance alerts**, and use AI as a supplement to – not a replacement for – regular inspections. The ASCE Code (Canon 1h) encourages embracing new technology but simultaneously *recommends caution with unfamiliar or untested tools* [2]. In practice, this means piloting AI systems carefully and comparing their predictions against expert judgment until confidence is warranted.

- **Aerospace AI and the Standard of Care:** In aerospace engineering, even small errors can be catastrophic. While advanced AI is being used for flight management and even design of aircraft (e.g., AI algorithms that helped design efficient rocket engines or lay out circuit boards), the **standard of care** in this industry is extremely high. Engineers should recall the ethical lesson from past automation issues: for instance, the automated control system (MCAS) in the Boeing 737 MAX was implicated in fatal crashes because of design flaws and inadequate pilot training. While MCAS was a conventional control logic rather than an AI, the ethical takeaways apply to AI as well: engineers must ensure that automated systems **don't introduce single points of failure**, that users/operators (pilots, in this case) understand the system's behavior, and that thorough testing and verification is done for all failure scenarios. No matter how advanced, an AI system's recommendations or actions **must be treated with professional skepticism and verified** to meet the rigorous safety standards that are the hallmark of mechanical and aerospace engineering.

4.3 Electrical & Computer Engineering

AI Applications: Electrical engineering and related fields (including computer engineering) utilize AI in areas such as **circuit design automation, power grid management, and electronics manufacturing**. For example, AI algorithms (often generative in nature) can assist in **microchip layout and routing**, optimizing circuit designs for speed and power efficiency far faster than manual methods. Neural networks are used in signal processing to optimize communication networks. The electric power industry employs AI for **smart grid** operations: forecasting energy demand, balancing loads, detecting faults, and even autonomously isolating parts of the grid during outages (an agentic AI function). In computer engineering and software, AI is increasingly used to generate code or system designs, and to manage complex IT infrastructure (like automated DevOps pipelines or cybersecurity systems that detect and respond to threats).



Figure 6. An engineer monitoring an agentic AI load management system that flags actions for human review.

Ethical Issues & Best Practices: Key considerations in electrical and computer engineering include:

- **Verification of AI-Designed Circuits and Systems:** When AI systems propose circuit designs (for example, an AI optimizing a printed circuit board layout or an FPGA configuration), engineers must thoroughly check these designs against electrical standards and performance requirements. A generative AI might produce a novel circuit that works in simulation, but the engineer is responsible for ensuring it meets electromagnetic compatibility rules, thermal limits, and doesn't introduce hidden failure modes. **Testing and validation remain crucial.** It would be unethical and professionally irresponsible for an electrical engineer to manufacture or deploy a circuit solely based on an AI design without review. All designs that will be fabricated should undergo the same scrutiny (simulation, prototype testing, peer review) as human-generated designs. This aligns with the idea that **engineers are responsible for every calculation or design they sign off, regardless of the tool used** [3].
- **Autonomy in Power Systems:** A modern electrical grid might use AI agents to manage distribution of electricity, especially with the rise of renewable energy (which can be intermittent) and smart appliances. These AI agents could autonomously react to changes – for example, by shedding certain loads, activating battery reserves, or rerouting power during a failure. Ethically, power engineers must ensure such agentic AI systems have been tested for all likely scenarios (and many “unlikely” ones). An error in an autonomous grid-management AI could lead to widespread blackouts or equipment damage. **Human oversight** is important, especially during initial deployment: engineers should be in the loop or at least “in the loop” (monitoring the AI’s decisions) until the system proves itself extremely reliable. Even then, periodic audits and simulations of “what-if” situations are necessary to ensure the AI’s control logic aligns with safe utility practices. Additionally, **cybersecurity and privacy** are crucial ethical concerns in this domain: if an AI manages critical infrastructure, it must

be protected against malicious attacks or manipulation. Engineers must work with cybersecurity professionals to safeguard AI-controlled systems so that they cannot be hijacked – an ethical imperative given the potential harm to the public from a compromised power or communications system.

- **Bias and Fairness in Algorithms:** In fields like communications or computer engineering, AI might be used to make decisions that affect users – for example, algorithms that allocate network bandwidth or manage traffic prioritization. If these algorithms are data-driven, they could inadvertently favor certain groups or uses over others. Engineers have an ethical responsibility to ensure that such systems are fair and do not unjustly discriminate. This might mean actively checking for bias in algorithmic decisions. For instance, if an AI scheduling algorithm in a telecommunications network learns to favor traffic from higher-paying neighborhoods at the expense of lower-income areas, that could be considered unethical unless intended and disclosed. While not a traditional “engineering” ethical concern in the sense of physical safety, **fair access and non-discrimination** align with the broader professional commitment to act in the public interest and treat all people fairly.
- **Software Engineering and AI-Generated Code:** Software engineering (often overlapping with computer engineering) is not always regulated by professional licensure, but many software engineers adhere to similar ethical principles, especially in safety-critical industries. With generative AI capable of writing code, ethical issues include **code quality, security, and intellectual property**. If a software engineer uses an AI like GitHub Copilot or ChatGPT to generate code for, say, a control system in a chemical plant or an embedded system in a medical device, the engineer must validate that code meticulously. There is a risk of bugs or security vulnerabilities in AI-generated code. It is unethical to deploy such code without thorough testing, as it could endanger users. Another issue is that generative code tools have been known to sometimes reproduce copyrighted code snippets from their training data. Utilizing such code without attribution or license could infringe intellectual property laws, putting the engineer and their employer at legal risk. Ethically, the engineer should review and rewrite AI-suggested code as needed to ensure originality and compliance with software licenses. Moreover, just as with any design, the engineer should document how the code was developed and tested, maintaining transparency in case of future audits or incidents.

4.4 Chemical & Biomedical Engineering

AI Applications: In chemical engineering, AI is applied to **process control, simulation, and materials discovery**. For example, AI controllers (agentic AI) can manage chemical plant operations by adjusting valves, temperatures, or pressures in real-time to optimize output and safety. Machine learning models predict equipment corrosion rates or optimize maintenance schedules for refineries. In chemical **and** biomedical fields, generative AI techniques help in discovering new materials or compounds (catalysts, drug molecules, battery materials) by predicting molecular properties and suggesting novel chemical structures. AI is also used for complex simulations in fluid dynamics and reaction engineering, sometimes creating surrogate models to approximate expensive calculations.

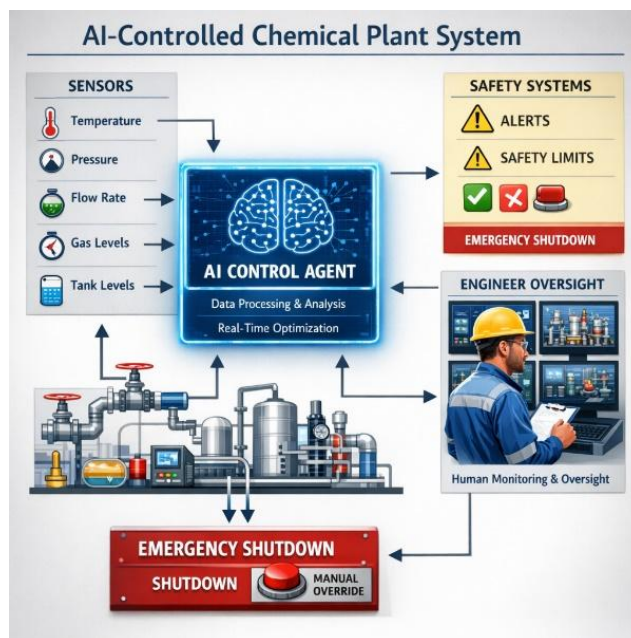


Figure 7. AI-controlled chemical plant system with safety limits, engineer oversight, and an emergency shutdown with manual override.

Ethical Issues & Best Practices: Chemical processes deal with hazardous materials and complex systems, so ethical use of AI focuses on preventing harm and ensuring compliance with regulations:

- Process Safety and AI Autonomy:** If an AI is given control of a chemical process (for instance, regulating a reactor in a chemical plant), any mistake could result in explosions, toxic releases, or other catastrophic events. Therefore, while an AI might efficiently keep a process within optimal parameters for yield, engineers must implement strict **safety interlocks and oversight**. Agentic AI in this domain should be constrained by safety limits – for example, an AI controller should never be able to exceed certain temperature or pressure thresholds, no matter what optimization it seeks. Human operators (engineers or trained technicians) should have the ability to **veto or override** AI decisions if something seems amiss. Additionally, regulatory standards (like OSHA’s process safety management standards or chemical industry protocols) likely require documented testing and human approval of control logic changes. Ethically, deploying an agentic AI in a chemical plant without exhaustive testing, simulated failure analyses, and a clear manual override procedure would be irresponsible.
- Validation of AI-Generated Formulations or Materials:** In research and development, chemical and biomedical engineers might use generative AI to propose new molecular designs (new drugs, polymers, nanomaterials, etc.). Ethical practice demands diligence in validation: an AI might suggest a compound that optimizes one property (say, strength of a material or efficacy of a drug) but the engineer must investigate side effects or other impacts (toxicity, environmental harm, manufacturability). For instance, if a generative model proposes a new chemical formulation for a high-strength polymer, the engineer should verify that the ingredients aren’t environmentally hazardous or banned substances. Releasing a new chemical product based purely on AI-generated

suggestions without proper lab testing violates the engineer's duty to ensure public and environmental safety. Moreover, there could be legal implications if the AI's design inadvertently replicates a patented chemical – another reason to thoroughly review and conduct patent searches when using AI for R&D.

- **Data Privacy and Consent:** In biomedical engineering applications of AI (such as AI-driven diagnostic tools or patient-monitoring systems), data ethics becomes paramount. Patient data used to train AI must be handled in compliance with privacy laws (like HIPAA in the U.S.) and with respect for patient consent. While this may go beyond typical engineering codes and into broader data ethics, a professional engineer working on a healthcare AI project should advocate for privacy and security measures as part of their commitment to the public's welfare. Any agentic AI that makes medical or health-related decisions (e.g., an AI that auto-adjusts medication dosages via a medical device) should be subjected to rigorous clinical testing and regulatory approval (FDA, etc.), and engineers have an ethical obligation to flag concerns if they feel an AI-driven medical device is not safe or effective.
- **Environmental Impact:** Chemical engineers must also consider the environmental implications of AI-driven processes. This includes both the direct impacts (does an AI optimization inadvertently increase pollutant output?) and the indirect **sustainability concerns** of AI itself (like the energy consumption of large AI models). While the latter is more of a global ethical issue, it aligns with the idea of sustainable engineering and the NSPE's admonition to be "faithful agents" for the welfare of the public, which can be extended to future generations. In practice, this means engineers should consider the carbon footprint of AI models they use (especially if running intensive computations or large cloud servers continuously) and weigh that against the benefits. If two AI solutions exist – one that uses a simpler model on local servers and one that relies on a massive cloud-based AI with heavy energy use – the engineer can ethically favor the more sustainable option, all else being equal, or press the company to mitigate the environmental cost (for instance, by using renewable energy).

4.5 Software & Systems Engineering

(Note: Software engineering is included here because generative and agentic AI are highly relevant to it, even though "software engineer" is not always a licensed PE in many jurisdictions. However, when software control systems intersect with public safety or critical infrastructure, professional engineers may be involved or similar ethical standards apply.)



Figure 8. A software engineer testing AI-generated code before deployment.

AI Applications: In software and systems engineering, AI plays dual roles: **as a tool for developers, and as a component within products.** Developers use generative AI to assist in writing code, generating test cases, or creating documentation. AI-driven tools can automate aspects of software design and project management (e.g., AI-based bug detection, effort estimation, or optimizing cloud resource usage). On the product side, software engineers build AI into systems – for example, developing a machine learning model that becomes part of a larger software system (like an AI module for fraud detection in a financial software, or a recommendation engine in a platform). Agentic AI in this field appears as **autonomous software agents** that perform tasks: think of automated trading bots, cybersecurity AI that identifies and neutralizes threats without human intervention, or *intelligent personal assistants* that perform actions on behalf of users.

Ethical Issues & Best Practices: Many ethical considerations in software mirror those already discussed (fairness, transparency, privacy, IP). A few noteworthy points:

- **Accuracy, Bugs, and Accountability:** If a generative AI tool writes a piece of code, who is accountable if that code fails? The answer, ethically and legally, is the **human engineer or the company** deploying it. Software engineers must treat AI-written code as if a junior developer wrote it – it requires thorough **review, testing, and verification.** There is an ethical obligation to ensure that software, especially if it controls physical devices or handles sensitive data, is **reliable and secure.** For example, if an AI helps generate the code for an insulin pump’s control algorithm, any bug could endanger lives. The responsible engineers must validate the code through code reviews, simulations, and testing to meet the standard of care for medical device software. This aligns with the general principle that engineers “*are also responsible for ensuring that AI-assisted work aligns with ethical and professional standards*” [3].

- **Bias and Fairness in Algorithms:** Software engineers working on AI algorithms must be aware of bias and discrimination. If developing, say, a loan approval algorithm or a facial recognition system as part of an engineering project, it's essential to test these systems for bias against any group. Unfair algorithms can cause real harm (e.g., denying services to certain populations) and erode trust in technology. Ethically, engineers should strive for fairness and equity – which can be seen as part of acting in the public interest and upholding the dignity and rights of all individuals. Techniques like fairness auditing of algorithms, diverse training datasets, and bias mitigation strategies should be part of an engineer's toolkit in the age of AI.
- **Privacy and Cybersecurity:** When software systems involve AI that collects or uses user data (from personal information in a smart city app to images from a public camera network analyzed by computer vision), respecting privacy is a key ethical (and often legal) duty. Engineers must incorporate data protection measures, ensure they only use data in ways agreed by users or consistent with privacy laws, and secure any AI systems against breaches. Professional ethics codes encourage compliance with the law and the "protection of the public." In modern terms, that includes protecting users' data from misuse or exposure, as data breaches can harm the public. It's recommended to follow frameworks like "privacy by design" when developing AI-infused software: build security and privacy considerations into every stage of development.
- **Intellectual Property & Plagiarism:** Software engineers should be cautious that generative AI may produce code that is too similar to existing copyrighted code (as noted earlier). Also, text-generating AIs might incorporate excerpts of documentation or literature without proper citation. Using such outputs without credit could violate ethical norms against plagiarism. Best practice is to use AI outputs as a starting point and then write your own final version, or clearly cite any substantial text that originated from another source. Some companies have guidelines or policies for AI use in coding – familiarize yourself with any such policy to ensure compliance.
- **Professional Accountability in Autonomous Decision-Making Systems:** When deploying agentic software agents (like an AI that autonomously makes trades or controls building systems), consider the potential impacts. While such systems might not physically harm people, they can have significant financial or safety implications. For instance, an AI managing building HVAC systems to save energy (an environmental engineering crossover) could inadvertently create indoor air quality issues if not properly configured – affecting occupant health. Software engineers should collaborate with domain experts (mechanical engineers for HVAC, financial experts for trading systems, etc.) to set appropriate constraints on the AI's actions. In all cases, there should be clarity on who oversees the agent's decisions and how to intervene if it behaves undesirably.

4.6 Environmental Engineering

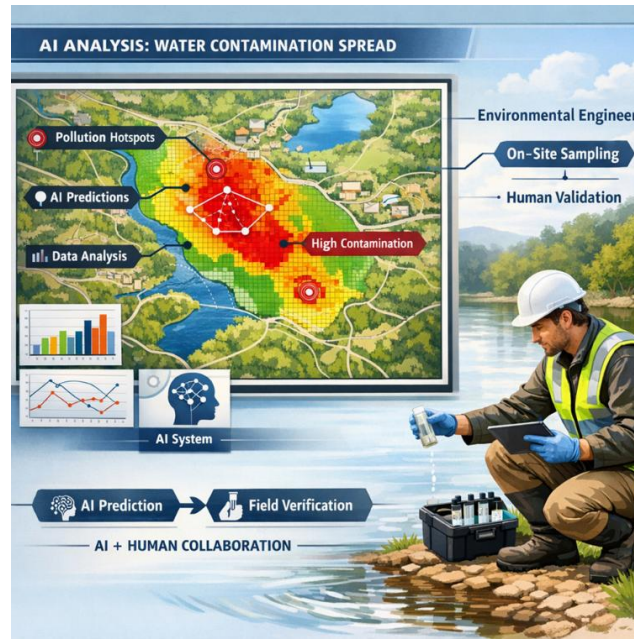


Figure 9. AI prediction of water contamination spread, verified by on-site sampling.

AI Applications: Environmental engineers use AI for **modeling and managing natural systems and resources**. This includes using machine learning for **climate modeling, pollution detection, environmental impact assessments, and resource management**. For example, AI can analyze satellite imagery to detect deforestation or oil spills (using computer vision to autonomously flag environmental damage – an agentic task), or optimize the operations of water treatment plants by adjusting chemical dosing in real-time. Generative AI might be used to model climate scenarios or to draft environmental reports based on large data sets of environmental measurements.

Ethical Issues & Best Practices: Environmental engineering often deals with public health and ecosystems, so the ethical use of AI ties closely to long-term public welfare:

- **Accuracy and Uncertainty in Predictions:** AI-driven environmental models (like climate projections, flood risk models, or air quality forecasts) are complex and inherently uncertain. Ethical use entails clearly communicating the **uncertainties and assumptions** in AI predictions. Engineers should avoid overstating the confidence of an AI model's prediction. For example, if an AI predicts a certain region is safe from 100-year flood risk, the engineer must double-check the data and possibly use multiple models to verify this claim. Misrepresentation of predictive certainty could mislead policymakers or the public, leading to inadequate preparation for environmental risks. Thus, honesty (avoiding deceptive assurances) and rigorous validation are critical. Wherever possible, engineers should compare AI model outputs with historical data and peer-reviewed scientific models, and update the AI models as new data becomes available.

- **Public Policy and Ethical Use of Data:** Environmental decisions (like where to build infrastructure or how to respond to climate change) often have significant societal implications. If AI is used to inform such decisions, engineers have an ethical duty to ensure the data and algorithms do not have hidden biases. For instance, an AI that prioritizes locations for environmental clean-up might inadvertently favor areas with more data (often wealthier regions) and overlook rural or underprivileged communities with less monitoring data. To prevent this, engineers need to recognize and compensate for data gaps. This aligns with broader ethical calls to ensure AI does not reinforce existing inequities [3].
- **Sustainability of AI Solutions:** Environmental engineers, in particular, are conscious of resource use and sustainability. It would be in contrast and unethical if an AI-driven solution to an environmental problem consumes disproportionate energy or resources. Engineers should evaluate the **environmental footprint of their AI**. For example, training a very large machine learning model on cloud servers can consume substantial electricity – if done using fossil-fuel power, it could indirectly contribute to carbon emissions. A balanced approach is needed: if an AI’s environmental benefits (e.g., optimizing energy use in buildings, reducing water waste) significantly outweigh its operational footprint, it’s justified, but if two solutions exist, the one with a smaller environmental impact might be the ethically preferable choice. This point reflects the expanding scope of “public welfare” to include environmental sustainability for future generations.
- **Case Example – AI in Environmental Remediation:** Consider an environmental engineer tasked with managing a contaminated site. They use an AI tool to predict the spread of a pollutant in groundwater and to optimize a remediation plan. The generative AI model suggests an approach that appears cost-effective by focusing cleanup on areas the model deems highest risk and forgoing certain regions. Ethically, the engineer must scrutinize this suggestion: Is the model possibly underestimating risk in areas with less data? Are there vulnerable communities downstream that the model failed to account for? The engineer should incorporate a **factor of safety** in environmental predictions as well, acknowledging uncertainties. Moreover, community engagement is part of ethical environmental practice – the engineer might use the AI output as a starting point but should also discuss with local stakeholders and consider social implications before finalizing the plan. The goal is to use AI’s power to inform and improve decisions, but not to abdicate the complex value judgments to a purely data-driven tool.

Module 5: Ensuring Ethical Use of AI — Guidelines and Best Practices

Across all disciplines, several **best-practice guidelines** emerge for the ethical utilization of agentic and generative AI in engineering. Engineers can use the following principles as a checklist when integrating AI into professional practice:

1. **Treat AI as an Assistant, Not an Authority:** Always remember that AI is a tool to support decision-making or design – *not a replacement for your professional judgment*. You, the licensed engineer, are the final decision-maker. As NSPE’s Board of Ethical Review noted, technology (from old CADD systems to modern AI) must not be used as a **substitute for essential engineering judgment** [1]. Use AI to enhance productivity and insight, but never to hand off your responsibility.
2. **Maintain Responsible Charge and Oversight:** Stay actively engaged with any task involving AI. Ensure that you understand how the AI is being used, and closely supervise its outputs. If an AI system is making autonomous decisions (agentic AI), implement **human-in-the-loop or human-on-the-loop controls** especially for high-risk operations. In practice, this can mean requiring human approval for critical decisions suggested by AI, or real-time monitoring of AI agents. Never sign or seal any document or design that you did not directly supervise simply because an AI produced it – doing so would violate the requirement that engineers only approve work done under their direction and control [1].
3. **Verify and Validate AI Outputs:** *Trust, but verify* every result from an AI. Just as you would check calculations done by a junior engineer, you must thoroughly check AI-generated calculations, designs, or recommendations. This includes:
 - **Cross-checking data and results** with independent methods or simplified models. For example, if an AI predicts a certain outcome, see if it makes sense via back-of-envelope calculations or traditional analysis.
 - **Physical testing or prototyping** for AI-designed components, when applicable, to ensure they perform as expected in the real world.
 - **Peer review or second opinions:** Having a colleague review an AI-assisted design or analysis can catch issues you might overlook, similar to reviewing any engineering work.

Always document how you validated the AI’s contributions – this documentation may be critical for demonstrating compliance with the standard of care if ever questioned.

4. **Know the Limits – Data and Algorithm Transparency:** Understand the general workings of the AI tools you use and their limitations. What kind of data were they trained on? Are there known failure modes or accuracy bounds? If the AI is a “black box” (its internal logic is not interpretable), use it with extra caution. Lack of explainability can be a red flag in safety-critical decisions [3]. Whenever possible, prefer AI tools that provide explanations for their recommendations, or use additional methods to interpret their results. Be ready to explain to others the basis of any AI-driven decision in terms they understand – this often means translating the AI’s output into conventional engineering reasoning.

5. **Guard Against Bias and Ensure Fairness:** Actively question whether an AI is treating all cases impartially. Biased data can lead to biased outcomes [3]. For instance, if using AI for deciding which infrastructure projects get priority, ensure the criteria are fair and not inadvertently favoring or disadvantaging a particular community without justification. Mitigate bias by using diverse training data and by testing the AI on a variety of scenarios. Ethically, this ties to the engineer's duty to be objective and to act as a faithful agent for *all* stakeholders, not just those who might be implicitly privileged by historical data.
6. **Protect Privacy and Confidentiality:** When using AI, especially third-party tools or cloud services:
 - **Do not upload sensitive or proprietary project data** unless you have ensured it will remain confidential (check the tool's privacy policy or use self-hosted AI solutions where data stays in-house). This protects client interests and complies with ethical directives to keep client information confidential [1].
 - Be aware of how the AI might use the data you provide. Some generative AI systems retain input data to improve their models, which could inadvertently leak information. Use sanitized or permission-cleared data whenever possible.
 - If AI is used to analyze personal data (e.g., in smart city projects or biomedical applications), ensure compliance with privacy laws and ethical norms regarding consent.
7. **Ensure Security of AI Systems:** For agentic AI especially, security is an ethical imperative. Protect AI systems from unauthorized access or malicious tampering. An engineer should consider threat scenarios: What if someone feeds false data to your AI (data poisoning) or hacks an autonomous system? This could lead to dangerous outcomes (imagine an attacker tricking an AI into misoperating the power grid). Thus, include cybersecurity experts in the design of AI systems for critical infrastructure, use secure coding and validation for AI software, and advocate for strong organizational policies on AI usage and data sharing [4].
8. **Continuous Learning and Training:** Given the fast pace of AI innovation, engineers have an ethical obligation to **stay educated** about new tools and their implications. Many engineers currently feel they lack preparation to handle AI-related ethical issues [3]. Seek out training (like this course) and stay updated with guidance from professional societies. NCEES and state licensing boards increasingly require or recommend ethics PDH credits; focusing on emerging technology ethics is a valuable way to fulfill these. Being informed helps you ask the right questions and spot potential problems early. Ethics training has been shown to make engineers *significantly more likely to recognize and appropriately respond to ethical issues* in the workplace [3].
9. **Communicate and Disclose Appropriately:** If AI was significantly used in your work product, consider informing your client or stakeholders. This doesn't mean every use of spell-check or simple automated calculations needs disclosure, but if, for instance, a feasibility study's conclusions were drawn from an AI data analysis, it may be wise to mention the use of the tool and describe the validation steps taken. This transparency can prevent misunderstandings and demonstrate professionalism. It also provides context in case the AI's output is later found flawed – everyone is aware that a tool was involved and that the engineer's role was to verify its results. Additionally, clear communication internally is crucial: if you are managing a team, ensure everyone understands how

AI tools should and should not be used on the project, and that they are aware of the ethical standards discussed here.

10. **Plan for the Worst-Case (Fail-Safe Design):** Just as engineers design physical structures with factors of safety and redundancies, AI systems should be designed and used with a **fail-safe mindset**. Expect that the AI can make mistakes. Ask “What is the worst that could happen if the AI is wrong or behaves unexpectedly?” then implement measures to prevent or mitigate harm in those scenarios. For example, an autonomous system should have an emergency shutoff; an AI-driven analysis should have a peer review or an alternative calculation method as backup; a data-driven model should have checks for data drift or anomaly detection to know when its predictions might no longer be valid. Preparing for AI failures is part of ethical risk management – you hope it never happens, but as an engineer you are bound to protect against foreseeable harm.

By following these guidelines, engineers can responsibly harness AI’s benefits—improving efficiency, exploring creative solutions, and handling complex data—while upholding the highest standards of ethical practice. The overarching theme is one echoed by both NSPE and ASCE: **AI does not diminish the engineer’s responsibility to the public; if anything, it raises the bar for diligence and ethical awareness** [3].

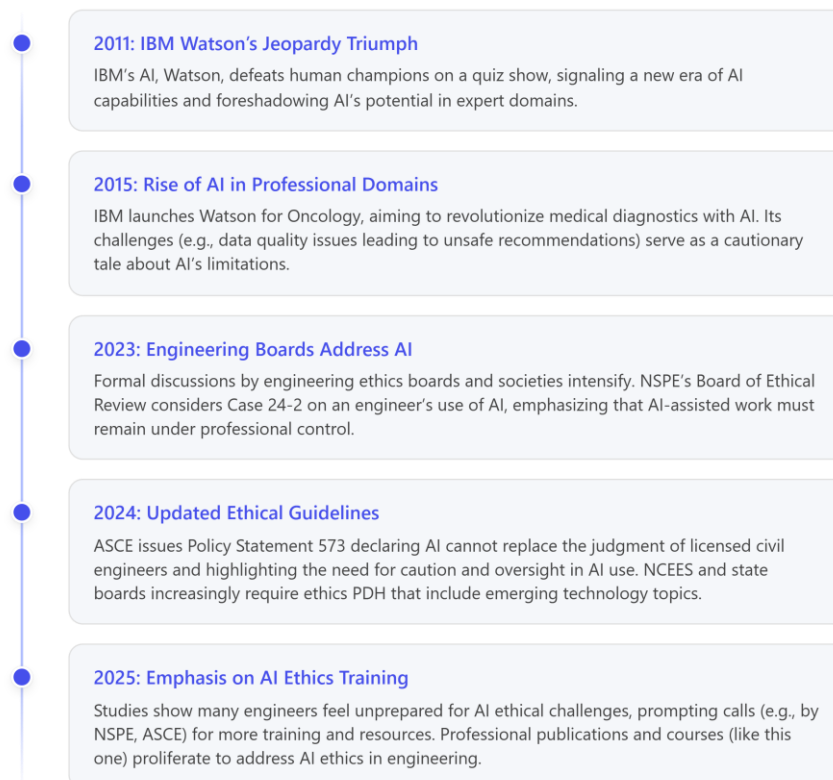


Figure 10. Timeline of AI milestones and ethical guidance in engineering, 2011 to 2025.

Module 6: Summary and Conclusion

Artificial Intelligence – in both its generative and agentic forms – is transforming how engineers design, build, and maintain systems. From civil and environmental projects to mechanical, electrical, chemical, and software engineering, AI is enabling powerful new capabilities and efficiencies. Generative AI can quickly produce designs and insights, and agentic AI can take autonomous action, but these advantages come with **ethical responsibilities and risks** that engineers must carefully manage.

Key takeaways from this course include:

- **Always prioritize safety and public welfare.** No matter how promising an AI-derived solution might appear, it must be rejected or reworked if it endangers health, safety, or welfare in any way. This is non-negotiable and at the core of the engineering ethos [6].
- **Stay within your competence and in control of the work.** Use AI in areas you understand well, and maintain direct oversight. Never allow AI to work unchecked or outside your domain of expertise while still expecting to sign off on the results [1]. The engineer is the final gatekeeper who ensures all output meets professional standards.
- **Use AI to assist, not to replace human judgment.** Welcome innovation and efficiency gains from AI – as encouraged by professional societies – but implement these tools in a way that *augments* your work rather than automating the ethical and decision-making roles that belong to you as a professional [3]. Technology can expedite calculations and offer insights, but it “**must never be a replacement or substitute for engineering judgment.**” [1]
- **Be vigilant about data and algorithms.** The quality of AI recommendations is only as good as the data and logic behind them. Watch out for biased or incomplete data sets, and for models that are “**black boxes**” lacking transparency [3]. Poor data or opaque algorithms can lead to errors and ethical pitfalls – from discrimination to dangerous designs. Always question how an AI arrived at its output.
- **Protect confidential and personal data.** When using AI, ensure you’re not inadvertently sharing sensitive information. Maintain confidentiality by using secure, approved tools or anonymizing data. This is part of being a faithful agent to your clients and employers and respecting privacy.
- **Ensure accountability and human intervention for agentic AI.** For autonomous systems, design them such that a human can intervene when needed and that the system’s actions are logged and traceable. *Accountability cannot be delegated to a machine* – ultimately, a professional engineer or responsible organization must answer for what an AI does. This is echoed in recent guidance that calls for identifiable human oversight even as AI autonomy grows [4].
- **Continue your ethical education.** The landscape of AI in engineering is evolving. Standards and best practices are being developed (e.g., new ISO/IEEE standards on AI ethics, NIST AI Risk Management Framework, etc.), and regulations will likely follow. Engaging in lifelong learning – through courses, seminars, or self-study – is crucial for staying current. This not only keeps you compliant with CPC requirements, but more importantly, it ensures you are well-prepared to navigate new ethical challenges. Research shows engineers with ethics training are far more confident and proactive in handling real-life ethical dilemmas [3].

In conclusion, the **ethical use of AI in engineering** is about balancing innovation with responsibility. By understanding what generative and agentic AI can do, and applying timeless engineering ethics principles to these new tools, you as a professional engineer can leverage AI to enhance your work while **safeguarding the public and upholding the honor of your profession**. This careful approach will help ensure that the integration of AI into engineering leads to better, safer, and more equitable outcomes, in line with the highest standards of professional practice.

References

1. NSPE Board of Ethical Review, “Use of Artificial Intelligence in Engineering Practice,” Case No. 24-2, National Society of Professional Engineers, July 2024. Analysis of an engineering ethics case where an environmental engineer used generative AI for writing reports and designing plans, discussing issues of competency, oversight, confidentiality, and disclosure. <https://www.nspe.org/career-growth/ethics/board-ethical-review-cases/use-artificial-intelligence-engineering-practice>
2. Hoke, T., “Mishandling AI Tools Puts Civil Engineers at Risk for Ethical Violations,” ASCE Civil Engineering Magazine, March/April 2025. Presents the case of IBM’s Watson for Oncology as a cautionary tale and extracts ethical lessons for engineers, including ASCE Code of Ethics Canon 1.h on considering new technology’s implications. <https://www.asce.org/publications-and-news/civil-engineering-source/civil-engineering-magazine/issues/magazine-issue/article/2025/03/mishandling-ai-tools-puts-civil-engineers-at-risk-for-ethical-violations>
3. Ellis, J., PE, “Engineering Ethics in the Age of AI: Protecting Public Safety While Using Emerging Technologies,” PDH-Pro, September 2025. Discusses professional obligations (NSPE and ASCE positions), key AI-related risks, and the importance of ongoing ethics training. <https://pdh-pro.com/pe-resources/engineering-ethics-in-the-age-of-ai-protecting-public-safety-while-using-emerging-technologies/>
4. Boinodiris, P., and Parker, J., “The Evolving Ethics and Governance Landscape of Agentic AI,” IBM Think. Explains the concept of agentic AI, the amplified risks of increased autonomy, and the need for robust governance and human accountability. <https://www.ibm.com/think/insights/ethics-governance-agentic-ai>
5. NCEES, Continuing Professional Competency (CPC) Guidelines, National Council of Examiners for Engineering and Surveying, 2021. https://ncees.org/wp-content/uploads/CPC_Guidelines_2021.pdf
6. International Institute of Building Enclosure Consultants (IIBEC), AI ethics article, May 2025. <https://iibec.org/wp-content/uploads/2025/05/2025-05-ai-ethics.pdf>