Ethical Implications of COBOT Implementation

C.J. Witherell, Grand Valley State University

CJ Witherell is a graduate student studying Product Design and Manufacturing Engineering at Grand Valley State University. Their undergraduate minor in philosophy inspired them to promote deep thinking, ethical reasoning, compassion, diversity, and equity-focused design within the engineering field. As the 2022 Wisner Engineering Fellow, they are developing a new product for Gentex Corporation in Zeeland, Michigan.

Ethical Implications of COBOT Implementation

CJ Witherell

Grand Valley State University

Abstract

The following paper explores new ethical considerations in the manufacturing industry that have arisen due to the advent of the fourth industrial revolution known as Industry 4.0. The concept of Industry 4.0 was researched to identify its impact on the manufacturing industry. One significant change of the era, namely the increased implementation of collaborative robots (COBOTs), was explored to determine the associated risks and their ethical ramifications. The risks of physical harm, cyber-attack, and electromagnetic interference-related malfunctions were identified and discussed, as well as their respective methods of risk mitigation. Then, the ethical implications were analyzed using the National Society of Professional Engineers (NSPE) Code of Ethics as well as the Utilitarian and Respect for Persons ethical frameworks. The rise in popularity of COBOTs in manufacturing has introduced the ethical responsibility to protect employees from new risks including physical harm during normal use and malfunctions due to cyber-attack and electromagnetic interference. Current and future engineers must be educated about the risks associated with COBOTs and their resultant ethical responsibilities.

1. Introduction

The concept of ethics has been explored for thousands of years, yet it seems to have gotten more muddled throughout the years as the world has become more complex. Still, it is important to recognize the significance and utility of the study of ethics in the modern world. Ethics is generally defined as the study of moral issues and decisions [1]. Life is full of decisions that can affect not just oneself, but the lives of others, and even the world. The study of ethics is about examining the proper balance and application of moral principles in everyday life. Ethics should be seen as a method of applying moral thinking, not an unchanging set of values [1]. In other words, the goal of the study of ethics is to improve one's ability to apply experience and reason to new situations to make the best possible decision.

It is especially important for engineers to have a basic understanding of ethics because the purpose of engineering is to serve society [2]. The focus on utility is what separates the field of engineering from fields like theoretical mathematics and the pure sciences. While other disciplines can remain in the conceptual realm, engineers are tasked with solving society's problems—typically through the use of technology. The job of an engineer often involves finding safer, faster, and/or cheaper ways to accomplish tasks [3]. Engineers should use their technical training and skills to make the world a better place. Unfortunately, engineering education is often so focused on the technical training it takes to become an engineer that the ethical training required to be a morally upstanding engineer is overlooked.

Engineers have ethical responsibilities to their employers, their employees, the environment, and the entire public. Often, the stakes of engineering projects are extremely high because people's lives depend on their success. The activities of engineers can have great impacts on the physical world around them and the beings living in it. Engineers do not exist in a bubble—they "exist and operate as a node in a complex network of mutual relationships with many other nodes" [2]. These complex relationships make it necessary to consider the impacts of decisions and actions on a range of parties.

The purpose of this report is to explore new ethical considerations that have arisen in the manufacturing industry due to the advent of the fourth industrial revolution known as Industry 4.0. Automation and connectivity have recently been increasing at a dramatic rate. It is important to take a step back and reevaluate the effects of these trends on the population to make sure that introducing Industry 4.0 is ethically justified. This evaluation will be conducted using the National Society of Professional Engineers (NSPE) Code of Ethics as well as the Utilitarian and Respect for Persons ethical frameworks.

2. Ethical Evaluation Methods

The National Society of Professional Engineers (NSPE) developed, and continues to develop, a Code of Ethics for Engineers. The goal of this document is to define and encourage

ethical conduct within the field of engineering. Though this code is intended to apply to professional engineers, engineers can look to it for guidance, regardless of discipline or rank. It provides statements of the fundamental duties of engineers, rules of practice that should be used to guide engineers' actions, and a list of professional obligations that engineers are bound to [4].

Two vastly different Western ethical frameworks will also be used to analyze engineers' ethical responsibilities. The first is Utilitarianism, which is a consequentialist ethical theory. In this framework, right and wrong are determined by the outcomes of decisions. Utilitarian methods of decision-making involve considering all the costs and benefits of different choices [5]. The best actions maximize utility, meaning that they promote the greatest amount of good for the greatest number of people. However, for the Respect for Persons ethical approach, it is the intent behind actions rather than their consequences that matters [5]. This approach requires that the autonomy, rights, and choices of all people be respected [5]. No one should be treated as merely a means to an end, so actions that deny individuals the ability to exercise their autonomy are wrong.

The NSPE Code of Ethics was chosen as an evaluation method since it applies to all engineering disciplines. It is the default reference document for professional engineers on issues of ethics. The Utilitarian and Respect for Persons frameworks were selected because they represent two ends of the spectrum. Due to the use of an often-numerical cost-benefit analysis, Utilitarianism is typically seen as an objective approach to morality. Since Respect for Persons requires an understanding of intent, it is understood to be more subjective. These two frameworks are often at odds with each other because they have distinctly different methods for justifying good actions. Discussing the concerns from all three of these perspectives should provide a thorough examination of COBOT-related ethics.

3. Industry 4.0 Background

Industry 4.0 is also known as the fourth industrial or technological revolution [6]. The first industrial revolution occurred between the end of the 18th century and the beginning of the 19th century. It involved the introduction of water and steam-powered mechanical manufacturing facilities. The second industrial revolution, which occurred a century later at the end of the 19th

century, was all about the introduction of electricity. This is when electrically powered mass production and the division of labor were established. The third industrial revolution, also called the digital revolution, took place between the 1960s and 1990s. The important change during this time was the introduction of electronics and information technologies. Making use of new digital technology, humanity began to automate manufacturing like never before.

These three industrial revolutions led to Industry 4.0, which is all about cyber-physical systems. This is the linkage of real objects and people with information-processing and virtual objects through information networks [6]. The new intelligent manufacturing environment involves the Internet of Things (IoT), increased automation, cloud computing, big data, system integration, and increased connectivity [7]. From an ethical responsibility perspective, one of the biggest changes has been the prevalence of robots created by engineers to work alongside people. This issue will be explored in depth in the following section of the report.

4. Ethical Considerations of COBOTs

4.1 COBOT Basics

The term COBOT is short for collaborative robot. A COBOT works alongside human beings and collaborates with them based on machine learning and human learning-based strategies [8]. COBOTs are especially useful for performing repetitive and tedious tasks, completing potentially dangerous tasks such as welding, transporting heavy or bulky parts, and handling small or intricate parts [9]. For example, in a manufacturing environment, a COBOT could assemble parts by screwing in the threaded fasteners—a task that requires consistency and precision but not considerable intellect. If the operator only needs to load the parts, that increases efficiency by leaving them available to complete other tasks. There have also been recent developments in robotic exoskeletons, which provide physical assistance to people [9]. When used in the manufacturing realm, these robots can help industrial workers by increasing their strength or endurance [9]. A symbiotic relationship between humans and robots can be extremely beneficial for manufacturing companies, but like with all matters, perfection is unattainable.

4.2 Physical Risks of COBOTs

Unfortunately, COBOTs can be a liability due to their inability to make moral judgments and the difficulties involved with assigning blame when things go wrong. In 1979, Robert Williams was working at a Ford Motor Company facility in Flat Rock, Michigan [10]. He was employed at the casting plant where the inventory system had provided erroneous values. Williams was tasked with scaling a large shelving unit to manually count and retrieve parts. While he was on the third level of the storage rack completing that task, a retrieval robot went to grab a part from the same area. It was too quiet for Williams to hear and too quick for him to react. Instead of grabbing the part, the robot struck him in the head. Williams was killed instantly. He was just 25 years old.

The Robert Williams case is the first death by robot on record [10]. Sadly, it is a perfect example of an unanticipated situation with a COBOT that resulted in the loss of life. The designers of the robot did not anticipate a human being in the area that parts were grabbed from, so they did not design it to avoid harm. The robot did not act maliciously, it simply acted. It was programmed to move and grab the part, so that is what it did. If the designers had considered that someone may be in the storage area, they could have implemented additional safety measures. The severity of the issue has only increased as robots have become more integrated into manufacturing. As they have become more prolific and capable, they have begun to work in even closer proximity to human beings.

4.3 Physical Risk Mitigation

Luckily, there are many ways to mitigate the risks of COBOTs including guarding, presence sensors, power and force limiting (PFL), and lockout-tagout procedures. One of the easiest and most popular methods to keep people safe from robots is simply to restrict their access. This can be done through physical guards or presence-sensing devices.

An interlocked barrier guard is a physical barrier that surrounds a robot as it works. It is composed of interlocking gates that are designed so that all the automatic operations of the robot

and its machinery stop moving when the connected gate is opened [11]. Safety switches are often used to sense when the gate is opened or closed. There are many types, but at the most basic level, there are two parts—a switch and an actuator. When the actuator enters or exits the specified range of the switch, the state changes. To restart the process, the gate must be closed, and it must be manually restarted from a control switch outside of the barrier so that the operator must exit the danger zone. Usually, a guard like this will prevent access from all directions with some sort of fence so that the robot's action is visible, but not accessible, which is perfect for a COBOT that lifts heavy objects or completes tasks like welding that could be dangerous to bystanders.

Similar to the interlocked barrier guard, a fixed barrier guard will physically restrict access to an area from all directions [11]. However, fixed guards require tools to remove. A fixed guard acts as a shield between the robot and the operators(s) or bystanders. They are a permanent part of the machine. For this reason, they are constructed of materials that can withstand the impacts of prolonged usage. It is the simplest type of guard, but the least flexible. They do not allow for quick modifications to the robotic technology and greatly limit collaboration prospects, so they are reserved for the most dangerous robotic operations.

The last type of physical guard is the least severe—the awareness barrier device. It simply defines a safety perimeter that makes people aware of a work area and prevents accidental entry into it [11]. Examples of awareness barrier devices would be railings, suspended chains, pedestrian barricades, and clear curtains because they do not prevent access to the hazard area, at least not from all angles. They are only advisable when the risk is low or fixed/interlocking barrier guards are impossible to implement. Because of this, awareness barrier devices work best for lower-speed robots with less dangerous tasks like loading machines.

Sensors can also be used to detect the presence of a person (or object) in a space where they should not be. Much like interlocked barrier guards, robot operations can be shut down, or slowed depending on the level of danger, when presence is sensed and not restarted until no presence is detected. There are three main categories of presence sensing devices, namely pressure mats, light curtains, and area scanners [11]. Pressure mats usually exist on the floor and are triggered by the weight of a person stepping into a hazardous area. Light curtains are a parallel

array of infrared light beams. The light beams are broken when someone reaches or steps into the field of beams. Laser scanners continuously emit an optical signal that scans across the detection range. Beams of light are sent out and the time it takes for the signal to return is measured. When a person enters the detection range, the measured time for the light to return to the emitter is less than usual, so undesired presence is identified. A similar function can be accomplished using ultrasonic scanners, where the light beam is switched out for a high-frequency sound beam. The range of these sensing devices can be adjusted to match the level of hazard. For example, the distance from the COBOT at which the presence is sensed could determine the degree of its speed reduction.

Due to the close interactions between humans and COBOTs, not all protective measures apply to each COBOT usage. Measures can be taken to place especially dangerous tasks behind interlocked or fixed barrier guards and those with greater risk could be shut down when presence is sensed. However, when people must work in close proximity to robots, or it is not possible to avoid human-robot contact, power and force limiting is necessary. In general, human beings naturally react to avoid collisions, but robots do not naturally react similarly. If a robot's path is obstructed and it is not specifically programmed to avoid doing so, the robot will collide with the obstruction. In the case of Robert Williams, this resulted in his death. PFL is an attempt to control a robot's motion to the point where it cannot seriously injure or kill a human worker. The robot should be programmed to perform a protective stop if a certain amount of force or pressure is exceeded while collaborating with humans [12]. Studies identified four different types of forces, namely impact force, clamping/squeezing force, pressure/surface pressing, and compression constant. An impact force causes elastic deformation of a person's soft tissue, meaning it is reversible when the force is removed. A clamping/squeezing force causes plastic deformation of a person's soft tissue, which means the tissue is permanently damaged. The pressure/surface pressing is the partial pressure load of impact and clamping/squeezing force when the contact area is small. The compression constant is the deformation constant of a region of the body, assuming linear deformation throughout the soft tissue [12]. Many studies were conducted to find the maximum allowable forces on parts of the body. For example, the larynx can take an impact force of up to 35 N, while the thigh can take up to 220 N [12]. Engineers must consider the parts of the body that parts of COBOTs might come in contact with and adjust the robot's speed, effective

mass, contact area, or contact duration to comply with these values. The robot is then programmed so that it will automatically stop itself if a force or pressure higher than the assigned limit is registered so that no further harm is done to the employee.

Still, even with all these safety measures in place, it is important to properly train employees. Part of the training process should be learning the safety policy, including which personnel are authorized to work with robots, what the proper safety procedures are, and where the safety procedures are posted [11]. Many companies already implement lockout-tagout systems to reduce the risks of harm during maintenance and repairs. This is a procedure rather than a safety device. First, hazardous energy sources must be isolated and shut down before work can be performed. Then, the power sources are physically locked, and a physical tag is placed on them that provides important information about who is responsible for the maintenance. The team member whose name is on the tag holds the key to the lock so that only they can remove the lock and start up the machine again. This is done to prevent the accidental powering of a hazardous machine while someone may be in the danger zone.

4.4 Electronic Vulnerabilities

The next problem is that electronics have introduced new vulnerabilities. Safety is about protecting people from the threats caused by robots; security is about protecting robots from the threats caused by external players [10]. Unfortunately, there are individuals looking to cause harm for personal gain, and modern criminals only need a computer. As the manufacturing world has modernized, more data is stored on computers, and more business is done virtually. This puts companies and their employees at a greater risk of cyber-attack than ever before. Inadequate security can allow COBOTs to be used to cause property damage and inflict harm on people.

The NotPetya malware attack took place in June 2017 [13]. It started in Ukraine and quickly spread around the world. The malware appeared to be extortionware, a traditional malware that infiltrates a company’s system and holds data, websites, or sensitive information hostage until certain demands are met. However, it actually deleted all of the master boot records so there was no way to recover the data, even when the ransom was paid. This attack affected a wide range of

sectors including manufacturing, finance, healthcare, energy, and government. It was estimated that the attack caused more than $10 billion in damages, making it one of the worst in history. Companies and their modernized manufacturing floors are at constant risk of cyber-attacks such as NotPetya. Sadly, there is no shortage of examples of cyber warfare.

Another less obvious external player is electromagnetic interference (EMI). EMI is a serious issue in the manufacturing environment. It presents a significant challenge to the normal operation of equipment, resulting in outright equipment lock-up, unpredictable tool behavior, software errors, erratic responses, parametric errors, sensor misreading, and component damage [14]. There are three major types of EMI: electrostatic discharges (ESD), parasitic emissions from equipment, and intentional emissions from equipment that use electromagnetic fields. The generation of electromagnetic fields is unavoidable in a manufacturing environment when tools are powered with electricity. Problems arise when the electromagnetic fields of different devices interact. Since EMI issues can cause systems to read incorrect values, the root cause is often difficult to identify. Identifying the presence of EMI is also rarely first on the troubleshooting checklist. When robots incorrectly interpret their inputs, doors open to a plethora of undesirable outcomes. The consequences of EMI can range from annoyances, such as glitching screens, to complete catastrophes.

In the late 1960s, EMI caused a huge incident with the first large-scale hovercraft testing tank [15]. A sophisticated overhead crane was designed to travel along the length of a bridge-like overhead structure called a gantry. The crane towed a hovercraft through a pool of agitated water. The team utilized resistor-transistor logic, running a 40V rail to mitigate the effects of noise. During the commissioning phase, the machine started up on its own. It began quickly traveling along the length of the pool without prompting. There was an emergency stop button, but it was at the operator's control position on the gantry. The workers could not run fast enough to catch it and press the button. The crane ignored all its limit switches and continued to hurdle across the pool. At the end of the track, it crashed through the wall at the end of the building. Fortunately, no one was harmed during the accident, but it could have caused a loss of life instead of just property damage. Following the disaster, it was determined that EMI caused the crane to believe it had received the start signal, and once it was moving, there was nothing that could have been done to

stop it. The system had to be rebuilt and, when it was, emergency stops were added all around the building and the team had to consider ways to reduce the effects of EMI.

COBOTs, along with any other automated components of assembly systems, are powered by electricity and controlled by computers. This means that, due to EMI, they could turn against employees at any moment. If they receive the wrong signal at the wrong time, robots could drop their heavy loads onto people, run full speed into workers, press down on someone's hand instead of a part, etc. The possibilities are endless.

4.5 Electronic Vulnerability Risk Mitigation

A focus on cybersecurity helps mitigate the risk of cyber-attack [16]. Accurate inventories of control system devices should be maintained and exposures of equipment to external networks should be eliminated. Hackers can exploit connections with external networks, so companies are encouraged to perform routine assessments of their systems to determine if any of these pathways exist. Next, networks should be segmented, and access should be restricted to specific groups. It is a good idea to limit access to resources based on role. Employees only need access to a fraction of the company's data to do their job and limiting access decreases vulnerabilities. This way, if one device or sector is compromised, the entire system is not. This is especially important in Industry 4.0, which is based on expanding the IoT. Firewalls can help segment systems because they filter the traffic between different parts of a network. The more segments and boundaries, the better. Virtual Private Networks (VPN) should be used to secure remote access to valuable information. However, the devices involved in the connection must also be secure, so each should be checked for malware. Of course, passwords should be strong and changed regularly. Finally, employees should be informed about the importance of cybersecurity so that they are motivated to participate in security measures and follow guidelines on all of their devices, including personal devices. For example, employees who are informed about phishing emails and phone calls designed to induce them to reveal private information are less likely to do so [16].

Like with cyber threats, the first step in mitigating the risk caused by EMI is education. Becoming aware of the problem and how it might manifest will reduce the likelihood of

catastrophic events. When undesirable circumstances are anticipated, security measures can be put in place. Beyond that, the solution to EMI is electromagnetic compatibility (EMC) [14]. EMC compliance is essential to a successful manufacturing environment. During installation, attention should be paid to the placement of equipment. Sensitive equipment should never be placed near high-energy tools, and they should not be on the same power and ground lines [14]. After maintenance, all grounds should be connected and covers/doors should be closed to decrease the probability of EMI events. Finally, frequent audits improve understanding of the manufacturing environment and encourage a proactive attitude toward EMC.

4.6 Ethical Evaluation

Clearly, there are pros and cons to the use of COBOTs in the realm of manufacturing. The first fundamental canon of the NSPE Code of Ethics states that engineers must "hold paramount the safety, health, and welfare of the public" [4]. Engineers often design robots that work alongside production team members with much less technical knowledge than the designers themselves. Most production workers are members of the public who did not attend years of schooling to learn about the risks introduced by robots. This makes it especially important to educate employees on cybersecurity measures and proper safety procedures such as lockout-tagout. They will be less likely to be harmed by COBOTs, harm others using the machinery, or put COBOTs at risk of cyber-attack if they understand the dangers. While enhanced connectivity may improve efficiency and morale, it also introduces more risk. Companies can decrease the likelihood of cyber-attacks by ensuring that employees follow the proper protocols. If a COBOT were to be hacked, or if it malfunctioned due to EMI, someone could easily be harmed, so according to the NSPE Code of Ethics, it is the duty of the designers to implement every possible safety measure. When safety is the primary objective in a manufacturing environment, people are much less likely to be harmed and they can go home to their families at the end of the day. A tangential effect is that, with fewer safety incidents, a company is more likely to stay in business and continue to employ individuals so that they can support their families.

The second fundamental canon of the NSPE Code of Ethics declares that "engineers shall perform services only in the areas of their competence" [4]. In other words, engineers should not

be making decisions or performing tasks for which they do not have the proper education and experience. If safety measures must be implemented by safety experts, then it follows that manufacturing firms are morally obligated to employ safety experts. Companies that fail to do so would not be doing their best to mitigate risk. Without the necessary expertise, safety measures may not be implemented correctly, or may not be implemented at all. An improperly installed light curtain, for example, may be as useless as no light curtain. Though all engineers should have a basic understanding of risk mitigation techniques, it is unrealistic to expect anyone to be an expert in *every* aspect of COBOT design and implementation.

From a Utilitarian perspective, they are highly recommended because they bring about more utility. Robots can complete many tasks faster than humans, can complete tasks that humans are incapable of completing, and can do so at all times without complaint or the need to take breaks. COBOTs bring a lot of benefits to companies, but the cost of their implementation is not simply the monetary cost of installation. Unfortunately, unanticipated situations and erratic behavior can make COBOTs a safety risk. Based on a keyword search, OSHA reported 49 robot-related workplace injuries between 1984 and 2022, 33 of which were fatal [17]. With just one reported accident in 2022, fortunately, as robot implementation in manufacturing has rapidly increased, the rate of robot-related injuries has not [17]. Though the injury rate has not yet slowed to a stop, this suggests that risk mitigation techniques are successfully being utilized in the manufacturing industry.

The question remains, is the increase in efficiency worth the increase in the risk of injury and loss of life? Ultimately, this question is problematic, and it highlights the key issue with cost-benefit analysis, which is that it is difficult to put a price on human health and life. What is certain is that it is the duty of engineers to anticipate unfortunate situations to the best of their ability and implement all relevant safety mitigation techniques in order to decrease the risk of harm to human beings. The best decision in a Utilitarian view is the one that produces the most net positive consequences, so if the harms are reduced through the methods previously discussed, then COBOTs are able to bring about more utility.

From a Respect for Persons standpoint, COBOTs are beneficial because they do not mind performing repetitive and tedious work. Oftentimes, people who work in manufacturing feel dejected because their job is to complete the same tasks over and over. They feel as if they are being used as a machine rather than a human being—in other words, as a means to an end. When COBOTs take over trivial positions, people's unique talents can be shifted to other positions that better respect their personhood. According to the Respect for Persons view, if a person's autonomy is not respected while they do their job, a robot can justifiably be used in their place. This also applies to a robot's ability to complete potentially dangerous and difficult tasks. If a person is put in harm's way during their job because they must use dangerous tools or lift heavy objects, then a robot should be used instead. Robotic exoskeletons can make tasks easier, resulting in healthier employees. They also allow for more diversity in the workplace because meeting certain height, strength, age, or background criteria would not be as critical. A COBOT can be designed specifically for tasks that are difficult for people to do and it can perform them consistently, decreasing the human safety risks.

However, robots that act erratically or cannot anticipate human behavior well enough are actively putting people in harm's way. This is wrong in the Respect for Persons view because a person's autonomy is not respected when they are hurt or killed by a robot. A person cannot consent to accidental harm via robot, and they cannot be forced to choose to work alongside a robot that may harm them. At this point, COBOTs are unable to make decisions based on moral reasoning. They cannot choose to not hurt someone because it is wrong; they can only avoid harm that they were programmed to be able to. Again, this leads to the conclusion that engineers must do everything they can to make COBOTs safe to work with.

An additional concern from a Respect for Persons standpoint is the collection of personal data. As the world becomes increasingly computerized, concerns about privacy are higher than ever. If a person does not consent to share their private information, then obtaining it would be a violation of their autonomy. Therefore, employers in an industrial setting must be honest with their employees about what information is being collected so that they may have informed consent. At this point, the robots in question are only capable of doing what they are programmed to do, so preventing the non-consensual collection of information is fairly simple. Still, the data alone is not

harmless. For example, COBOTs currently collect cycle time data on individuals. This data could be used to correlate efficiency with age, gender, etc., which may be used to generalize about groups of people or even justify hiring biases. When artificially intelligent systems inevitably integrate into the manufacturing field, the focus should be on limiting what information can be gathered (especially without consent), deeply considering what information should be permitted to be obtained, and deciding what can be done with that information.

Another important ethical issue when using COBOTs is with determining who is at fault when accidents do occur. In a case where accidental EMI causes a robot to behave erratically, who should be blamed—the robot designers, the individual who introduced the interfering device, the robot itself, etc.—and what should the consequences be? In a purposeful EMI or cyber-attack, the attacker is clearly at fault, but can the designers be held responsible for being unable to anticipate and prevent the attack? When it comes to issues like this, blame is often spread between multiple parties, which decreases the amount of responsibility accepted by individuals. Ultimately, each case is unique, and developing a standard method for assigning blame is unrealistic. It comes down to deciding what risks are expected to be anticipated and prevented.

Despite engineers' best efforts, there will always be risk. COBOT designers cannot be expected to anticipate every possible failure mode or attack. Fortunately, the International Organization for Standards (ISO) provides helpful tools for mitigating COBOT-related risks. When designing COBOTs, engineers can turn to the ISO/TS 15066:2016 document, which specifies the safety requirements for collaborative industrial robot systems [18]. More broadly, ISO 31000 was designed to "help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment" [19]. As the ISO puts it, "failure to manage risks is inherently risking failure," and the stakes are highest when human lives are at risk. Therefore, it is crucial to follow these standards. Dedicating time and effort to anticipating the worst-case scenario takes much of the blame off engineers when something inevitably goes wrong. It is the responsibility of all engineers to ensure that safety standards focused on human well-being are the driving force of design decisions. Failure modes and effects analysis (FMEA), the implementation of risk mitigation techniques, frequent audits, and honest reporting of accidents are critical to COBOT safety and success.

5. Implications for Engineering Education

In response to an increasing cultural concern with ethics, the subject began to emerge as a theme in academia in the 1980s [20]. A pivotal moment in engineering education was the release of the first edition of the textbook *Ethics in Engineering* in 1983. Co-written by an engineer, Roland Schinzinger, and a philosopher, Mike Martin, the book addresses moral issues within and surrounding engineering [20]. Since the 1980s, ethics has become increasingly integrated with engineering education. In 2000, the Accreditation Board for Engineering and Technology (ABET) added "an understanding of professional and ethical responsibility" to its list of required educational outcomes [21]. However, a standard methodology for its instruction has never been established, and engineering students still receive a range of exposure to ethics. The primary method of engineering ethics education has historically not been the philosophical reflection proposed by Schinzinger and Martin but rather the analysis of specific case studies and codes of ethics [20]. This approach has unfortunately led to a "mismatch between faculty and student perceptions of ethics" [22]. As faculty attempt to convey the importance and nuances of ethical reasoning, students see a list of codes and rules to memorize [22]. While that approach may provide a good foundation, studies show that students are not fully meeting the intended learning outcomes [22]. Experts argue that programs should provide broader approaches that emphasize individual responsibility as well as public policy and institutional obligations [23, 24].

To reach true understanding, students must critically examine the importance of engineering in their field [20]. Ethics should be reconceptualized "as an integrative force rather than a discrete requirement" [22]. Students should actively participate in their ethics education, and it should not be separate from their engineering education. It must be relocated "from the periphery of the curriculum to its core by empowering students to investigate ethics in the ways that are most meaningful to them" [20]. A proven methodology for doing so is a "modified version of the Critical Incident Technique (CIT), which asks students to locate an ethical problem in a film, text, or TV program, and then briefly to describe the problem, analyze its ethical dimensions, and indicate possible responses" [20]. Students may even be able to draw from personal industry experience or interview a professional engineer to identify a problem. This paper discussed a set

of cases that may be relevant in controls, computer, and electrical engineering courses, but these cases are not representative of the entire field of engineering. Repetition of the ethical evaluation approach used in this paper—analyzing a range of cases from multiple perspectives—will cultivate engineers that are better equipped to tackle ethical issues in their field.

6. Conclusion

This report explored new ethical considerations in the manufacturing realm due to the rise in popularity of collaborative robots, or COBOTs. The risks of physical harm can be mitigated through guarding, sensors, power and force limiting, and lockout-tagout procedures. The risks of cyber-attack can be mitigated by segmenting networks, establishing firewalls, ensuring secure remote connections, and encouraging strong passwords. The risks caused by electromagnetic interference can be mitigated with proper grounding, informed placement of equipment, and routine auditing. The NSPE Code of Ethics, the Utilitarian ethical framework, and the Respect for Persons ethical framework all support taking these aggressive measures to keep people safe. As Industry 4.0 continues to increase automation and connectivity, it will only become more important to make efforts to ensure the safety of those in manufacturing environments. Future engineers must be educated about the importance and complexity of ethical reasoning so that they are prepared to evaluate current and future ethical issues related to Industry 4.0 and beyond.

7. References

[1] W. T. Lynch and R. Kline, "Engineering Practice and Engineering Ethics," *Science, Technology, & Human Values*, vol. 25, no. 2, pp. 195–225, Apr. 2000, doi: https://doi.org/10.1177/016224390002500203.

[2] J. M. Basart and M. Serra, "Engineering Ethics Beyond Engineers' Ethics," *Science and Engineering Ethics*, vol. 19, no. 1, pp. 179–187, Jul. 2011, doi: https://doi.org/10.1007/s11948-011-9293-z.

[3] D. Trentesaux and E. Caillaud, "Ethical stakes of Industry 4.0," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 17002–17007, Jan. 2020, doi: https://doi.org/10.1016/j.ifacol.2020.12.1486.

[4] "Code of Ethics for Engineers," Jul. 2019. [Online]. Available:

https://www.nspe.org/sites/default/files/resources/pdfs/Ethics/CodeofEthics/NSPECodeofEthicsforEngineers.pdf

[5] C. Witherell, "Team Analysis of the Bhopal Disaster," Unpublished Coursework, EGR 602, Grand Valley State University, Grand Rapids, MI, 2022.

[6] T. Devezas, J. Leitão, and A. Sarygulov, Eds., *Industry 4.0*. Cham: Springer International Publishing, 2017. doi: https://doi.org/10.1007/978-3-319-49604-7.

[7] A. C. Pereira and F. Romero, "A review of the meanings and the implications of the Industry 4.0 concept," *Procedia Manufacturing*, vol. 13, pp. 1206–1214, 2017, doi: https://doi.org/10.1016/j.promfg.2017.09.032.

[8] F. Chromjakova, D. Trentesaux, and M. A. Kwarteng, "Human and Cobot Cooperation Ethics: The Process Management Concept of the Production Workplace," *Journal of Competitiveness*, vol. 13, no. 3, pp. 21–38, Sep. 2021, doi: https://doi.org/10.7441/joc.2021.03.02.

[9] V. Leso, L. Fontana, and I. Iavicoli, "The occupational health and safety dimension of Industry 4.0," *Med Lav*, vol. 109, pp. 327–338, 2018, doi: https://doi.org/10.23749/mdl.v110i5.7282.

[10] L. A. Kirschgens, I. Z. Ugarte, E. G. Uriarte, A. M. Rosas, and V. M. Vilches, "Robot hazards: from safety to security," A*rXiv*, Sep. 2019, Available: https://arxiv.org/abs/1806.06681

[11] *Occupational Safety and Health Administration*, United States Department of Labor, 21 Sept. 1987, www.osha.gov/enforcement/directives/std-01-12-002.

[12] Falco, Joe, et al. *Collaborative Robotics: Measuring Blunt Force Impacts on Humans*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=912089.

[13] U. Tatar, B. Nussbaum, Y. Gokce, and O. F. Keskin, "Digital force majeure: The Mondelez case, insurance, and the (un)certainty of attribution in cyberattacks," *Business Horizons*, vol. 64, no. 6, pp. 775–785, Nov. 2021, doi: https://doi.org/10.1016/j.bushor.2021.07.013.

[14] Kraz, Vladimir. "EMI Issues in the Manufacturing Environment." *Conformity*, Jan. 2007, pp. 38–42.

[15] "Cranes can suffer dangerous EMI – EMC Standards,"

www.emcstandards.co.uk. https://www.emcstandards.co.uk/cranes-can-suffer-emi2 (accessed Mar. 27, 2022).

[16] "10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks," 2016. [Online]. Available: https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf.

[17] "Accident Search Results Page | Occupational Safety and Health Administration osha.gov," *www.osha.gov*. https://www.osha.gov/ords/imis/accidentsearch.search (accessed Apr. 2, 2023).

[18] ISO - International Organization for Standardization, "ISO/TS 15066:2016," *ISO*, Mar. 8, 2016. https://www.iso.org/standard/62996.html (accessed Mar. 30, 2022).

[19] "ISO - ISO 31000 — Risk management," *ISO*. https://www.iso.org/iso-31000-risk-management.html/

[20] C. Mitcham and E. E. Englehardt, "Ethics Across the Curriculum: Prospects for Broader (and Deeper) Teaching and Learning in Research and Engineering Ethics," *Science and Engineering Ethics*, Aug. 2016, doi: https://doi.org/10.1007/s11948-016-9797-7.

[21] "ABET Engineering Criteria 2000," *user.eng.umd.edu*. https://user.eng.umd.edu/~zhang/414_97/abet.html (accessed Nov. 04, 2022).

[22] M. E. Sunderland, "Using Student Engagement to Relocate Ethics to the Core of the Engineering Curriculum," *Science and Engineering Ethics*, vol. 25, no. 6, pp. 1771–1788, Apr. 2013, doi: https://doi.org/10.1007/s11948-013-9444-5.

[23] J. R. Herkert, "Future directions in engineering ethics research: Microethics, macroethics and the role of professional societies," *Science and Engineering Ethics*, vol. 7, no. 3, pp. 403–414, Sep. 2001, doi: https://doi.org/10.1007/s11948-001-0062-2.

[24] C. Mitcham, "A historico-ethical perspective on engineering education: from use and convenience to policy engagement," *Engineering Studies*, vol. 1, no. 1, pp. 35–53, Mar. 2009, doi: https://doi.org/10.1080/19378620902725166.