NSF/ASME Design Essay Competition 2025

Graduate Submission

Anaheim, California

From Autonomy to Empathy in Manufacturing

Integrating Bio Signals and Voice UIs for Secure, Human-Centric Manufacturing

Advisor: Dr. Beshoy Morkos

University of Georgia

Runu Proma Das

Emily McCollum

From Autonomy to Empathy in Manufacturing

Integrating Bio Signals and Voice UIs for Secure, Human-Centric Manufacturing

Abstract

The rapid advancement in manufacturing towards autonomous, AI-driven systems unlocks innovation opportunities but also introduces new cybersecurity challenges ranging from identity mismanagement to deepfake data-driven engineering. As high-tech enterprises transition to 2040, prioritizing human-centric collaboration is essential to address these risks while improving productivity and workers' well-being. This essay explores a multi-modality solution integrating electrodermal activity (EDA) and voice user interfaces (VUIs) to shape the future of high-tech manufacturing enterprises by 2040. EDA is a non-invasive bio-signal that offers real-time insights into an operator's cognitive workload, stress, and emotional state to support human health and performance. VUIs offer hands-free, intuitive control driven by AI authentication to counter deepfake threats and ensure secure human-AI interactions. Combining physiological monitoring with voice command technologies plays a pivotal role in ensuring seamless, secure, and unique human-machine communication. This multi-layered approach will support not only industry productivity and ergonomics but also strengthen cybersecurity resilience in human-machine collaboration.

1. Introduction

The manufacturing sector is currently integrating Industry 4.0 (I4.0) technologies such as Internet of Things (IoT), big data analytics, Artificial Intelligence (AI), cloud computing, and Cyber-Physical Systems (CPS). IoT allows machines and devices to communicate, share information, and carry out activities without the need for active human intervention. Integrating big data analytics and cloud computing is essential to analyze data in IoT environments. These technologies enable the extraction of valuable insights, process optimization, and provide enhanced computational capacity, data processing capabilities, and collaborative tools for remote resource access. AI imitates human intelligence in computers, enabling the systems to have the power of human thinking, reasoning, learning, and problem-solving processes to perform tasks [1].

The I4.0 shift has transformed how high-tech companies operate, focusing on automation and efficiency in production systems [2]. However, I4.0 has its limitations as companies move forward towards the year 2040, such as its heavy reliance on automation at the expense of workers' well-being, contributing to cognitive fatigue and stress, and its vulnerability to cybersecurity risks, including data breaches and deepfake manipulations. These limitations indicate that I4.0 is not enough to maintain competitiveness in an increasingly dynamic global economy, which is why companies should focus on integrating Industry 5.0 (I5.0) to redefine industry success in 2040.

Unlike I4.0's technology-driven focus, I5.0 emphasizes human-centered, focused on human collaboration between workers and industrial systems. This industry shift prioritizes sustainability, resilience, and ethical technology use, addressing the limitations of I4.0 while incorporating competitive advantages. For high-tech companies, adopting I5.0 will be essential to thrive in the year 2040, where human potential, adaptability, and security are crucial.

To be a successful high-tech enterprise in 2040, companies must incorporate an intuitive interface for human-centric design, such as voice user interfaces and real-time psychological monitoring to mitigate fatigue and enhance decision-making, ensuring workers remain integral to advanced systems [3].

2. **Addressing Challenges and Supporting Literature for Industries in 2040**

With the rise in interconnection systems, human-AI collaboration must be secure through robust cybersecurity measures, authentication, and encryption to protect against threats such as deepfake audio or identity mismanagement [4]. Equally critical are decentralized operation technologies such as blockchain, used in decentralized autonomous organizations (DAOs), which enables secure global collaboration while safeguarding intellectual property [5]. Adaptive systems further enhance competitiveness by responding dynamically to the operator's needs, such as cognitive and physiological states, through real-time monitoring and environmental shifts, to facilitate the best practice for human well-being in 2040 high-tech industries. This section of the essay provides the background of the core concept and outlines the challenges associated with it.

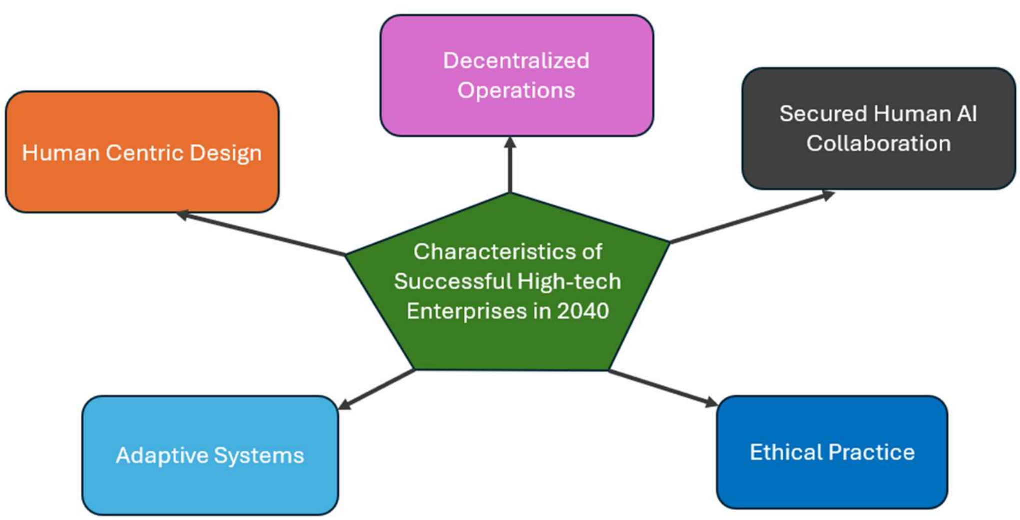

Fig. 1: Characteristics of a Successful High-tech Enterprise in 2040

2.1 **Human-Machine Collaboration Practice**

Industry 4.0 has driven a continuous growth of advanced technologies. All these technologies are developing the next generation of manufacturing, introducing Industry 5.0. In the next generation, manufacturing is data-driven, which requires efficient communication between all machines and sensors, and humans. Human Machine Interface (HMI) is defined as the interaction between humans and machines (e.g., sensors, robots, etc.) where humans can communicate, monitor, and control the automated system through digital interfaces such as tabs, dashboards, virtual and augmented reality. A well-established HMI is important to next-gen manufacturing due to understanding and predicting system usability and status. HMI is developing with integrated AI and real-time data visualization and analysis to enhance its capability under uncertain situations [18, Parasuraman]. With the rise of I5.0, HMI is also evolving with human physiological and psychological cues with direct commands.

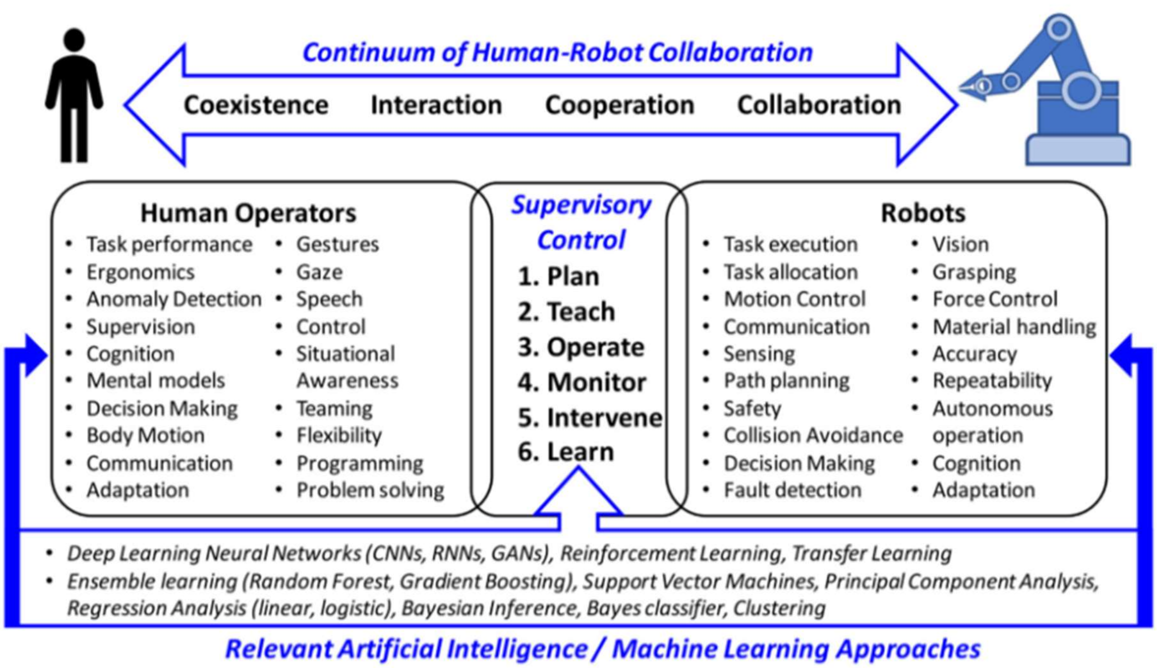

Fig. 2: Demonstration of common Human and Machine interaction [6]

2.1.1 Bias and Human Oversight in HMI

Automated systems and AI systems are trained based on historical data. which can introduce biases if not carefully managed. If the systems are designed and trained based on some stereotypical human behavior patterns, such as male operators being assigned to the creative tasks, or female operators being assigned to repetitive tasks, can convey an incorrect message to the system if any changes occur. In addition, the training of AI algorithms needs to be based on a clean dataset, otherwise, bias cannot be avoided due to an insufficient or inaccurate dataset. Moreover, the next generation manufacturing plant creates multiple dashboards, which can be harder for an aged employee; however, the systems could expect the same output from the An aged employee, analyzing their working efficiency history. Operator literacy and age-based tech familiarity are often oversights during the design of new technology infrastructure, which affects the overall productivity of the industry [7].

2.1.2. Limited adaptiveness of new tech, unsafe interruptions

The AI system is trained based on a traditional dataset, which sometimes lacks variability and unpredictable patterns in data. With the next generation of manufacturing, industry aims to perform based on real-time events where continuous variables, unstructured datasets are common, which is a limitation of trained automated systems. While systems are being automated for optimized productivity in the manufacturing industry, any unpleasant collapse of the system or unexpected bottleneck in the system requires manual intervention, which exposes unsafe interruptions. This kind of scenario introduces errors, sometimes malfunctions in the automated algorithms. Moreover, all technologies are connected to an internet server; any disruptions, such as annual maintenance or cyberattacks, can restrict the optimal connectivity, and in-time responsiveness is a major risk in the production rate of a company [8].

2.2 Text-to-speech, speech-to-text detection human and AI transform message

As high-tech manufacturing transitions towards I5.0, the integration of physiological monitoring highlights the need for intuitive and secure interfaces to enhance human-AI collaboration. Text-to-speech (TTS) and speech-to-text (STT) technologies are crucial in this shift to enable seamless communication between operators and cyber-physical systems. TTS converts text inputs into spoken output, allowing machines to deliver real-time instructions, while STT systems process spoken commands to control equipment or verify user identity. These technologies create efficient, hands-free interactions in automated environments, but also introduce the cybersecurity challenge of detecting AI-generated deepfakes and misinterpreted audio [9]. STT systems, such as voice user interfaces (VUIs) allow operators to issue hands-free commands to machine tools, reducing the physical strain and improving safety in hazardous manufacturing environments. Robust voice recognition models can classify multiple verbal commands in noisy factory settings with high accuracy. Most of these systems operate offline to minimize reliance on STT engines and to enhance cybersecurity by reducing external vulnerabilities [10] . Factory noise can degrade voice recognition accuracy, and the rise in AI-generated speech poses the risk of unauthorized commands or data manipulation. Misinterpreted or fake commands can lead to operational errors, equipment damage, and safety hazards for workers [9]. To address those challenges, STT systems are incorporating AI-detection to differentiate human and deepfake audios, and machine learning models (MLMs) analyze voice patterns to identify anomalies to achieve accurate, real-time AI-generated speech detection. This capability is essential for authenticating operators in secure environments, preventing deepfake audio from triggering undesirable and unauthorized actions. Integrating these systems with physiological monitoring can enhance security by cross-validating voice inputs with biometric data to ensure only authorized personnel can control machines.

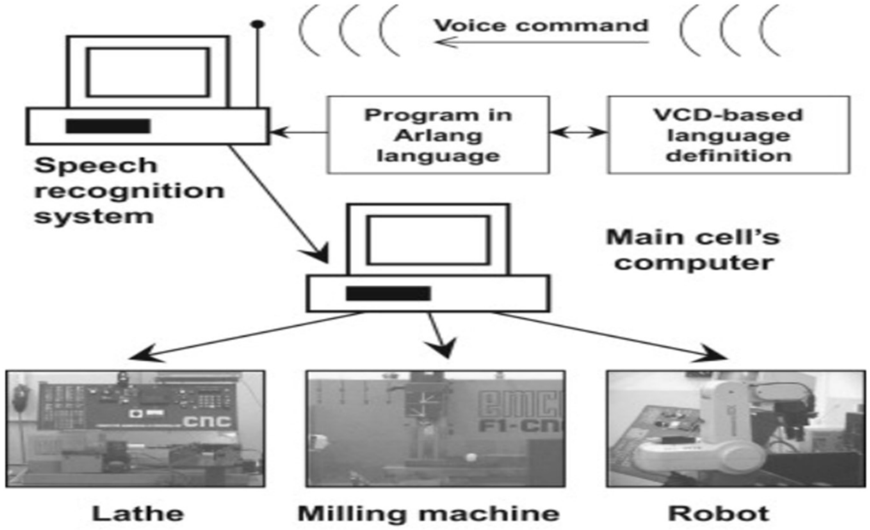

Fig.3: Speech-to-Text Transition with Machines [8]

2.2.1. Deepfake literature on industry

The rise of I4.0 with Industrial Internet of Things (IIOT) interconnects many industries together through cloud and other modern technologies, which increases the potential for cybersecurity risks. The lack of identity (e.g., human, AI bots, etc.) robustness and control of accessibility to CPS is a major concern. Traditional authentication methods (e.g., password, PIN code) are an easy target for identity theft. The failure of correct identity detection can result in inappropriate task assignments. Though large enterprise companies have taken initiatives to authenticate identity through RFID or biometric factors, the system remains complicated. The complicated authentication raises privacy issues, which are an obstacle to deployment [11].

However, the integration of TTS and STT technologies in high-tech manufacturing emphasizes the need for secure human-AI interactions to counter threats such as AI-generated deepfake audio. In I5.0, human-centric collaboration drives a company's operational success, so deepfakes pose the significant risk of enabling unauthorized commands or data manipulation that could potentially disrupt production or compromise intellectual property (IP). Deep fake audios are AI-generated mimics of human voice that can bypass traditional authentication systems, allowing malicious actors to issue unauthorized instructions to the CPSs and extract sensitive information.

In manufacturing, operational errors or safety hazards from misinterpreted or misleading commands can lead to serious consequences. To address this, identity detection mechanisms are emerging as solutions to ensure secure and authentic HMIs in industrial environments [5], [12].

Current research illustrates the severity of deepfake threats and proposes countermeasures in a manufacturing setting. Deepfake audio can undermine supply chain communications or manipulate control systems, which can lead to costly disruptions or safety violations. For example, a deep-fake voice command could trigger a robotic arm to perform hazardous actions that endanger the workers or damage the equipment. Identity detection systems counter this by using MLMs that identify anomalies in the voice patterns to distinguish human speech from AI-generated speech. These systems can be enhanced by integrating physiological monitoring to cross-validate voice inputs with biometric data to ensure only authorized operators' access to critical systems.

On the other hand, the security of automated systems, such as robotic arms, robots, requires to be assured. Manipulation of any designed control system, targeted by hackers towards data, can collapse the whole manufacturing plant. To improve productivity, safety, and job satisfaction, industries aim to develop user-friendly systems and intuitive interfaces and improve human-technology interactions.

2.3 **Physiological State Integration Literature**

Multitasking, repeated tasks, and environmental factors (such as temperature and noise) all contribute to human fatigue and cognitive load in manufacturing, which has a detrimental effect on output and decision-making. Complex interfaces brought about by more contact with robots and AI as automation progresses can overwhelm workers, resulting in mental exhaustion, decreased interest, and even injury from incorrect orders and insufficient training [5], [6], [13].

2.3.1. Electrodermal activity (EDA) technology Overview

'Electrodermal activity' (EDA) is a term used to trace the changes in the electrical properties of skin resulting from the autonomic nervous system. Its principle is based on human sweat glands that are managed by the sympathetic nervous system. The nervous system activates the "fight or flight" response and is the only neurological system that has control over these glands. EDA can provide both psychological and physiological measures at the same time. Several studies have illustrated that EDA is highly correlated with self-reported emotional arousal [14].

The data from the EDA is generally a small and constant voltage for two electrodes placed in human skin. Skin conductance level and response are two main components of the EDA data. EDA, along with Photoplethysmography (PPG), measures heart rate through blood volume in tissue. With the advancement in personalized settings in the human factor field, portable EDA devices have become popular. Multiple options, such as ring-mounted Mood metric, wrist-worn

E4, EdaMove, sensor-based Emotibit, are available on the market. This technology has been used in various fields such as clinical diagnosis, psychological and physiological studies, biofeedback, consumer behavior analysis in the marketing field, and so on.

3. Proposed Solution for 2040 Industry

To address the challenges of cybersecurity, operator fatigue, and complex human-AI interactions, the integration of electrodermal activity (EDA) and voice command systems offers a promising dual-modality approach to the growing complexity in next-generation manufacturing in 2040. The dual modality approach can enable real-time safety, communication, and adaptation in human and AI collaboration environments. By combining EDA's insights into the operator's well-being with VUIs and decentralized authentication, this solution aligns with the evolving demands of global production systems.

3.1 EDA with machine learning integration:

EDA has the capability of being a physiological marker of human cognitive workload, stress, and affective state. It is a non-invasive signal acquisition system that can recognize human mental fatigue, cognitive load, and stress in real time. EDA with machine learning can provide continuous feedback on an operator's physiological state based on their working speed and response to immediate decision-making. For instance, any operator is monitored and found as stressed; possibly, a trained robot can take over for a couple of hours to ensure the operator's well-being. This personalized approach will not only improve user performance, long-term well-being of the workforce, precision in automation, and informed protocols but also enhance risk management of cyber-attacks in next-generation manufacturing.

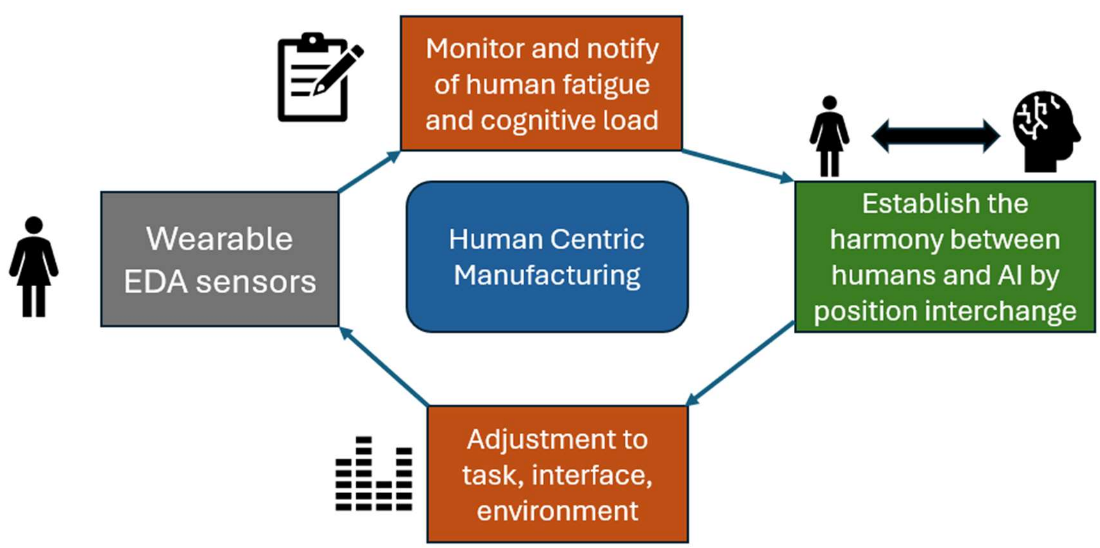

Fig.4: Bio-signal (EDA) integration in Next Gen manufacturing

3.2 Voice Command Interface: Building on EDA's insights, voice user interfaces (VUIs) enable hands-free, intuitive control in cyber-physical manufacturing systems. The next manufacturing generation emphasizes seamless interaction between humans and machines. While most HMIs are manual, VUIs are a subset of HMIs that allow operators to input spoken commands to equipment, which reduces physical strain and improves safety in hazardous manufacturing environments [4]. Current voice recognition models demonstrate robust performance in identifying and classifying multiple commands in noisy factory settings [2]. Cross-validating voice inputs with EDA data will ensure that only authorized personnel can control the machines to mitigate risks. VUIs can also monitor an operator's fatigue by analyzing voice tone alongside EDA signals to trigger task adjustments, preventing errors and enhancing productivity.

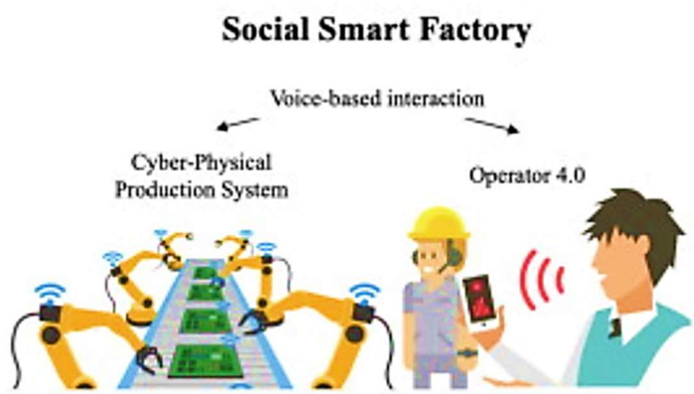

Fig. 5: Voice Command Activation Process [15]

3.3 Decentralized autonomous organization: The usage of centralized authentication methods is vulnerable to single-point failures. As our proposal for the 2040 high-tech industry involves multi-modal sensitive data, the centralized method will be inflexible and can blur the benefit of the advanced system. On the other hand, Decentralized approaches such as DAO that use blockchain-based frameworks allow high-tech enterprises to distribute authentication processes across multiple networks to improve resilience against cyberattacks. A proposed cryptographic and special token-based framework could ensure secure voice data exchange to protect against addressed deepfake manipulations while maintaining scalability across decentralized operations [1]. This approach aligns with I5.0's focus on secure, human-centric collaboration, enabling global contractors to interact safely without exposing IP. By 2040, integrating these identity detection systems with TTS/STT technologies and EDA will create a multi-layered security framework to ensure authentic human-AI interactions and minimize operational risks.

4. **Advanced Preparation**

4.1 Personalized Human Centric Approach

- *Customized EDA with industry standards meets*

To enter I5.0, human well-being needs to be served promptly in an industry setting. Based on our proposal, the initial step to well-being could be to operate the bio-signal sensors and devices and create an infrastructure for an industrial environment. The current bio-sensing devices are designed for clinical and research purposes, which limits their ability to match harsh industrial constraints (e.g., noise, dust, temperature). For the beginning step, the existing personal protective equipment (PPE), such as forearm work jackets, can be adapted to cover the wearable devices while acknowledging industrial constraints.

Additionally, raw bio-sensing data is usually noisy with unique variability. To meet the industry standard bio-sensing data where operators' stress, attention, and workload can be detected, resilient and strong machine learning models are required. These models could convert these bio signals into actionable cognitive state estimations to facilitate in the long run. Moreover, after having a meaningful dataset with bio-sensing signals, an explainable AI (XAI) can be trained to ensure the transparency of cognitive state detection

- *Voice Command Integration Preparation*

Complementing EDA's physiological insights, VUIs require strategic preparation to ensure secure and intuitive human-AI interactions. Enterprises should invest in developing company-specific command libraries tailored to their manufacturing processes and tasks to enable precise control of cyber-physical systems in noisy environments. These libraries can incorporate AI-driven detection to identify human fatigue or stress through VUI analysis and be cross-validated with EDA data. To accelerate adoption, partnerships with leading voice detection companies can provide access to their recognition models and offline processing capabilities to reduce cybersecurity risks. Developing interactive dashboards for bidirectional voice communication can streamline operations and reduce cognitive overload by allowing the operators to issue commands and receive synthesized feedback via TTS. Additionally, virtual reality (VR) based training simulations can familiarize workers with VUI systems. This training can incorporate scenarios of deepfake detections and false ID authentication to build operators' proficiency. By prioritizing these steps, enterprises can create a robust VUI ecosystem that supports I5.0's human-centric and secure collaboration goals.

4.2 System Robustness

The high-tech industry requires resiliency and robustness in the system. Implementation of human centricity is possible by defining system configurations. Using multi-AI agents, a standardized design for autonomous systems, real-time information sharing between humans, and a strong decentralized network can be established to ensure a secure system in next-gen manufacturing. With the integration of the features of I5.0, the necessity of AI model auditing is compulsory. Incorporating physiological data can be achieved by ensuring fairness, accountability, and bias mitigation. The infrastructure of AI models needs to provide vulnerability identification to differentiate actual signals and cyber risks.

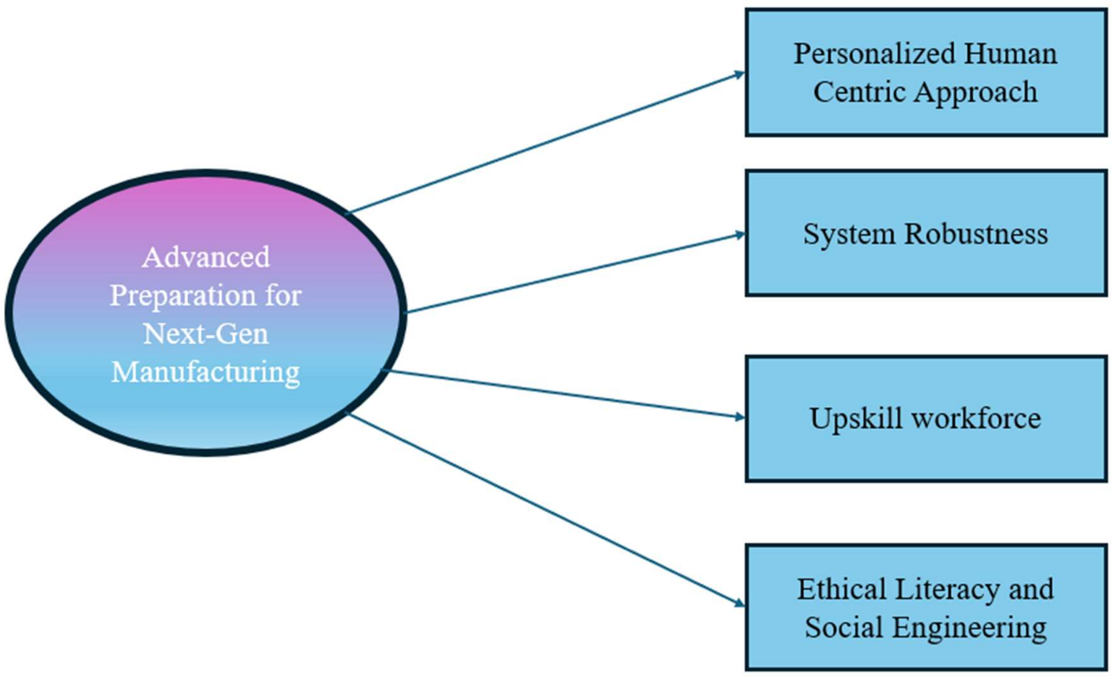

Fig. 6: Advanced Preparation for the 2040 industry

4.3 Upskill Work Force

Before beginning any addition to the existing I4.0, undoubtedly, an upskilled workforce plays an essential part. The training of employees (e.g., engineers, maintenance and safety personnel, line operators) in industry is the foremost necessity. Moreover, the future generation workforce must be trained with hands-on and software-based skills (e.g., model training, simulation practice) to be ready for the next generation manufacturing industry. These skills can be embedded in curricula, and labs can be designed with augmented and virtual reality systems so that students in colleges can experience real industry scenarios. On top of all of these, the partnership with industry and colleges in terms of bootcamps, certification programs, and research projects could strengthen the workforce. In addition, by ensuring the proper training of the workforce, AI supervision jobs can be created for the next generation of manufacturing.

4.4 Ethical Literacy and Social Engineering

Finally, the importance of ethical literacy and social engineering practice cannot be unnoticed. By 2040, the industry will incorporate human physiological data, and literacy and transparency are required. Through informed consent forms, data privacy rights, some indicators of data collection can be designed with the policy-making companies (e.g., ISO 27001 Compliance, OSHA) to empower this process. Multiple campaigns regarding deepfakes, personal data ownership, cyber scams, and attacks can be the initial step to facilitate empowerment. It is mandatory to ensure that the employees know that personal data, such as physiological data, is safeguarded and only collected for supportive purposes.

Conclusion

As manufacturing industries develop towards human centricity and smartness, integrating human physiological features such as EDA activities and voice commands will be essential to provide a safeguarded environment. These technologies have the potential to transform industries into environments that not only increase productivity but also respond empathetically to human states. To ensure this adaptation in the future, robust systems, sensor-based infrastructure, a trained workforce, and ethical literacy are required to preserve human trust and dignity. With this kind of assurance, high-tech enterprises in 2040 can be shaped around safety and harmony in human and machine collaboration, ensuring long-term success.

Acknowledgement of Using AI

We used only generative AI to assist in framing and fine-tuning ideas during the drafting process of this essay which are cross-checked to ensure accuracy.

References:

[1] J. F. Arinez, Q. Chang, R. X. Gao, C. Xu, and J. Zhang, "Artificial Intelligence in Advanced Manufacturing: Current Status and Future Outlook," *Journal of Manufacturing Science and Engineering, Transactions of the ASME*, vol. 142, no. 11, Nov. 2020, doi: 10.1115/1.4047855.

[2] C. Zanoli, V. Villani, and M. Picone, "The Road to Industry 5.0: The Challenges of Human Fatigue Modeling," in *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 4797–4804. doi: 10.1109/SMC53992.2023.10394500.

[3] E. R. Stepanova *et al.*, "Designing with Biosignals: Challenges, Opportunities, and Future Directions for Integrating Physiological Signals in Human-Computer Interaction," in *DIS 2023 Companion: Companion Publication of the 2023 ACM Designing Interactive Systems Conference*, Association for Computing Machinery, Inc, Jul. 2023, pp. 101–103. doi: 10.1145/3563703.3591454.

[4] S. Răileanu, F. Anton, T. Borangiu, S. Anton, and M. Nicolae, "A cloud-based manufacturing control system with data integration from multiple autonomous agents," *Comput Ind*, vol. 102, pp. 50–61, Nov. 2018, doi: 10.1016/j.compind.2018.08.004.

[5] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F. Y. Wang, “Decentralized Autonomous Organizations: Concept, Model, and Applications,” *IEEE Trans Comput Soc Syst*, vol. 6, no. 5, pp. 870–878, Oct. 2019, doi: 10.1109/TCSS.2019.2938190.

[6] C. Brady, S. Sawant, K. C. Madathil, and N. McNeese, “A Systematic Review on the Effect of Cognitive Fatigue in Teams,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Sep. 2024, doi: 10.1177/10711813241275515.

[7] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, “A Model for Types and Levels of Human Interaction with Automation,” 2000.

[8] A. Rogowski, “Industrially oriented voice control system,” *Robot Comput Integr Manuf*, vol. 28, no. 3, pp. 303–315, Jun. 2012, doi: 10.1016/j.rcim.2011.09.010.

[9] A. Mukherjee, J. Mertes, M. Glatt, and J. C. Aurich, “Voice User Interface based control for Industrial machine tools,” in *Procedia CIRP*, Elsevier B.V., 2024, pp. 121–126. doi: 10.1016/j.procir.2023.09.238.

[10] O. Aydogmus, M. C. Bingol, G. Boztas, and T. Tuncer, “An automated voice command classification model based on an attention-deep convolutional neural network for industrial automation system,” *Eng Appl Artif Intell*, vol. 126, Nov. 2023, doi: 10.1016/j.engappai.2023.107120.

[11] E. Othman and R. Mahafdah, “Recalibrating Human–Machine Relations through Bias-Aware Machine Learning: Technical Pathways to Fairness and Trust,” *Journal of Posthumanism*, vol. 5, no. 4, Apr. 2025, doi: 10.63332/joph.v5i4.1091.

[12] M. Wazid, A. K. Mishra, N. Mohd, and A. K. Das, “A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact,” *Cyber Security and Applications*, vol. 2, Jan. 2024, doi: 10.1016/j.csa.2024.100040.

[13] A. Adem, E. Çakit, and M. Dağdeviren, “Occupational health and safety risk assessment in the domain of Industry 4.0,” *SN Appl Sci*, vol. 2, no. 5, May 2020, doi: 10.1007/s42452-020-2817-x.

[14] B. U. Cowley and J. Torniainen, “A short review and primer on electrodermal activity in human computer interaction applications,” Aug. 2016, [Online]. Available: http://arxiv.org/abs/1608.06986

[15] F. Longo and A. Padovano, “Voice-enabled Assistants of the Operator 4.0 in the Social Smart Factory: Prospective role and challenges for an advanced human–machine interaction,” *Manuf Lett*, vol. 26, pp. 12–16, Oct. 2020, doi: 10.1016/j.mfglet.2020.09.001.

[16] Grammarly and Gemini, GPT 4.0 and 4.5

Appendix

We utilized various generative AI tools such as Gemini, GPT 4.0 & GPT 4.5 to cultivate and structure our ideas. These tools enhanced our understanding of concepts. Using a Chat GPT Plus account, we had access to limited Chat GPT 4.5 usage. Chat GPT 4.5 is labeled "*Research Preview*" and says it is good for writing and exploring ideas, thus, we started with this model to get the key concepts to focus our solution around. This model provided a detailed breakdown of our questions, much more than what we used, however, it gave a lot of insight into the possible applications and challenges that were used to brainstorm how to apply these insights into a productive and safe solution. Chat 4.0 helped refine our ideas and find potential papers that applied to the key concepts of our solution. We encountered some hallucinations when it came to the sources provided by Chat GPT 4.0, but they were quickly caught and disregarded. We also briefly explored the Gemini 2.5 Flash model, which turned out to be quite insightful. One of its standout features was its ability to present a clear-thinking process, guiding us toward thinking aloud. Additionally, it provided supporting resources for the information it shared, which helped us trust its responses and reduced concerns about hallucinations.
We did not use any output verbatim to make sure the originality and avoid plagiarism. Every suggested paragraph was carefully reviewed, fact-checked, and written in our own words. Additionally, to enhance clarity and correctness, we occasionally used Grammarly for minor language refinements.

Overall, the tool acted as a collaborative assistant, helping us think more critically about our writing and exploration. It also helped us to save time on research in a structured way. The final essay reflects a combination of our understanding, manual research, and meaningful revisions of AI-assisted suggestions.