Tailoring MLOps Techniques for Industry 5.0 Needs

Csaba Hegedűs, Pál Varga
Department of Telecommunications and Media Informatics
Budapest University of Technology and Economics
2 Magyar Tudósok krt., Budapest, Hungary, H-1117
Email: {hegeduscs, pvarga}@tmit.bme.hu

***Abstract*—It is a very popular era for machine learning (ML) applications, and Industry5.0 aims to have AI as one of its key technologies. Still, only a few ML initiatives make it to a production-grade implementation, mostly due to lacking proper Continuous Integration and Delivery framework and MLOps practices. This is especially true for industrial use cases, where the trust and reliability of ML applications are mission-critical. Most of these applications fail during the final stage of the development lifecycle, i.e. acceptance testing and validation of the ML application, while being integrated into Cyber-Physical System of Systems (CPSoS). This paper explores the key requirements for deploying ML applications in industrial scenarios, emphasizing the critical role of Digital Twins, edge AI, and responsible-explainable AI techniques in ensuring efficient and responsible operations. Building upon previous models, this paper suggests two process models: (i) the Olympics model for MLOps-coupled CPS engineering and (ii) the MLOps engineering toolchain for industrial applications.**

I. Introduction

The Industry 5.0 paradigm brings together the power of smart manufacturing with advanced Machine Learning (ML) applications to revolutionize industrial processes, especially with human-machine collaboration [1]. However, a large number of ML projects fail, with many proofs of concept never progressing into production due to the lack of appropriate DevOps practices established [2]. In this paper, we present an overview of ML Development and Operations (ML DevOps) techniques tailored to Industry 5.0 use cases, discussing their potential impact on enhancing productivity, sustainability, and safety in industrial environments.

MLOps is an emerging discipline that aims to streamline and optimize the end-to-end lifecycle of Machine Learning (ML) models, from development to deployment and maintenance. It borrows concepts and practices from DevOps, a set of software engineering practices that emphasizes collaboration, automation, and monitoring throughout the software development cycle. MLOps focuses on addressing the unique challenges faced in deploying and managing ML models, such as version control of data and models, model (concept) drift, and reproducibility. By automating model training, testing, and deployment, MLOps should (in theory at least) enhance model deployment speed, reliability, and scalability, making it easier for organizations to deploy and manage ML applications in production environments [3].

ML-based solutions are already used in industrial operations, from design and operations [4] to smart maintenance and quality control [5]. Clear requirements for ML applications in industrial scenarios, particularly in the context of (i) Digital Twins (DT), (ii) various Edge AI applications, and (iii) Responsible and Explainable AI research, that are becoming crucial for achieving efficient and effective operations in Industry 5.0 scenarios. These are a couple of industrial use-case-specific requirements that make ML application introduction a bigger challenge in this domain.

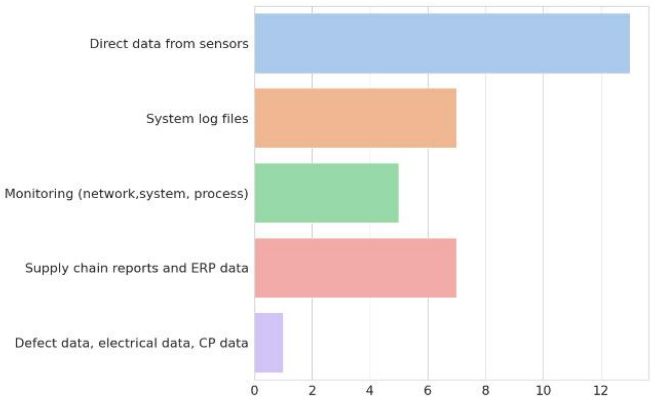

Fig. 1. Industrial data sources in AIMS5.0 project

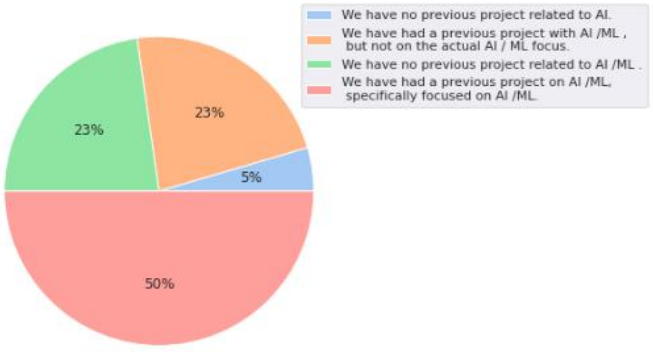

Fig. 2. Experience with ML Ops in AIMS5.0 project

As a current example, within the European AIMS 5.0 KDT-JU research project [6], 53 consortium partners have been asked in 20+ industrial use cases about MLOps and ML

978-3-903176-59-1 ©2023 IFIP

applications in current endeavours. Based on their answers, it is clear that while ML and AI applications are desirable, yet they still face issues around data availability, ML architecture and MLOps practices, as depicted by the results of this project's internal survey, see Figures 1, 2.

The primary purpose of this paper – based on the AIMS and research literature surveys – is to tailor and customize Machine Learning Operations (MLOps) practices to meet the specific requirements and challenges posed by Industry 5.0. Chapter II collects requirements and presents supporting data from AIMS 5.0 research project, Chapter III discusses relevant ML Ops practices and technologies. Chapter IV proposes an integration architecture for ML Ops practice in Industry 5.0 scenarios and Cyber-Physical System of Systems engineering (CPSoS) [7]. Chapter V concludes the paper.

II. Requirements for MLOps in Industrial Use Cases

The industrial domains each – such as manufacturing, production, logistics, aerospace, health etc. – have somewhat different expectations for ML integration and tool sets than consumer applications and services or the ICT domain. While the functional targets are similar – e.g. prediction, classification, knowledge extraction, object detection, or speech recognition – there are further non-functional requirements that present additional challenges. These stem from various aspects of safety, security and privacy of data, sovereignty, explainability, real-time synchronization of digital twins, or resource optimization in distributed, heterogeneous (and potentially edge deployed) environments, just to name a few.

Digital Twins [8] have emerged to become a cornerstone technology in Industry 5.0, acting as virtual replicas of physical assets or processes. These digital replicas enable real-time monitoring and analysis, significantly improving maintenance, troubleshooting, and performance optimization. For ML Ops purposes, DTs essentially allow ML models to leverage real-time (hopefully complete and accurate) data for better decision-making. Ensuring synchronization between the digital twin and its physical counterpart is vital for accurate predictions and effective model training. Regarding AI-driven application examples of Digital Twins in smart manufacturing and advanced robotics, Huang et.al. [9] provided a very comprehensive survey. This study categorizes the objectives of AI-driven DTs as productivity, availability, and quality, in all sorts of application areas from production planning to material processing and predictive maintenance, as well as from sensing of novel indicators to XaaS and business models.

With the proliferation of IoT devices and the need for real-time processing and decision-making, ML algorithms are to be deployed at the network edge, closer to the data source, since industrial scenarios often demand real-time decision-making and they are often latency sensitive. Moreover, mission-critical data often cannot leave on-premises due to its data quantities or for business security reasons. The Edge AI paradigm addresses these challenges by deploying ML models directly on edge devices, reducing reliance on cloud-based solutions and minimizing data transmission delays. In Industry 5.0, Edge AI is supposed to empower decentralized MLOps, enabling autonomous systems and supporting real-time analytics at the network's edge. Ensuring the robustness and security of edge AI models are also critical factors in maintaining the integrity of MLOps in industrial applications.

Meanwhile, the Responsible AI paradigm is another key consideration in the deployment of ML applications in industrial scenarios. Responsible AI frameworks and techniques address biases, interpretability, and ethical concerns associated with ML algorithms. In the context of Industry 5.0, responsible AI practices need to ensure that ML models are designed and deployed in a way that respects human values, privacy, and safety. This includes considerations such as the explainability of ML models, data privacy, and the impact of these applications in the cyber-physical production network [4].

A similar paradigm called Explainable AI (XAI) also holds significant importance for industrial use cases where transparency and trustworthiness of AI systems are crucial. First and foremost, XAI demands models that provide human-understandable explanations for their predictions and actions. Transparent model architectures and feature importance rankings are essential to comprehend the reasoning behind the AI's decisions. Moreover, contextual explanations that consider the specific industrial process, data, and domain knowledge are vital for users to trust and validate AI-driven outcomes [10]. These are all related to the safe cooperation between humans and machine cooperation for Industry 5.0 use cases.

These requirements all tie back to the CPS nature of industrial automation: the output of the models is to be utilized in producing various goods and services by operating machinery. Currently, ML and AI applications are getting incorporated into initiativesthat raise high expectations on MLOps methods,procedures [11], safety and security compliance [12] and engineering tools to support manufacturing [13] throughout the organization – or even among organizations. These then limit the true iterative, trial-and-error nature of DevOps and MLOps practices that can be included.

III. Related Works

A. MLOps Overview

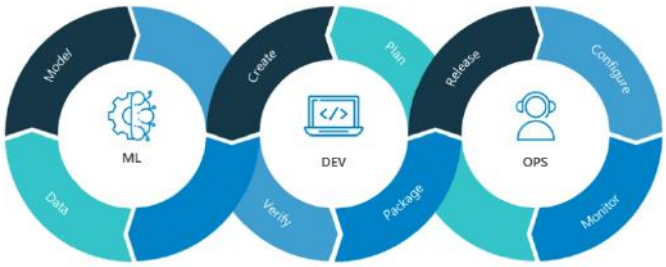

Fig. 3. MLOps is often visualized as an extended DevOps model [14]

Machine Learning Operations have been extensively researched over the last few years. It is considered an extension of DevOps practices while focusing on the data engineering and ML engineering prospects, as depicted in Fig. 3. This work assumes the ML Ops taxonomy, practices and framework described in various surveys: [3], [15], [16], [17]. Based on these and general industrial experience, nearly all ML-based application includes three main artifacts: Data, ML Model, and surrounding Code. Corresponding to these artifacts, the typical machine learning project consists of main phases:

- Data Engineering: data acquisition & data preparation with ETL-like pipelines [18],
- ML Model Engineering: data exploration, ML model training and
- Code Engineering: integrating ML model into the final product, i.e. packaging, serving and monitoring.

However, not all ML projects reach the final operationalization stage, i.e., packaging and deployment of the ML application for continuous serving. While there is a plethora of design patterns and examples that support this phase, the majority of the cases do not integrate and validate the ML application in real-time production traffic. These projects get s̈tuckät various steps of the development progress. This also happens to industrial research use cases, since there not only the ML application development and MLOps process that are inadequate, but the surrounding CPSoS architecture is usually evolutionary as well.

Regarding the tool-chains of MLOps best practices, this work considers the surveys of [15] and [19] for a good overview, among others. However, it is worth noting that these tools and ML best practices primarily focus on creating new, customized ML models from custom data, and serving on local, private or public cloud deployments, handling the whole DevOps lifecycle of these developments. However, the ML industry is slowly moving towards a different business model: in the last couple of years, ML-based commercial products (e.g., ChatGPT, Bard, Midjourney) or open source projects such as Huggingface have started to emerge.

These SaaS (Software-as-a-Service) applications are now prevalent around us. Agility, convenience, simplicity, scalability, and security are the key drivers behind the adoption or migration to SaaS applications, whereas full control and high customizability are the top reasons organizations stick to self-hosted and self-managed deployments. These SaaS companies offer ready-made models for specific goals and offer great experience out-of-the-box in the domains of, among others:

- Computer vision: object and face recognition, classifications, picture enhancement, etc.
- Audio processing: classification, noise reduction, pattern recognition, etc.
- Natural Language Processing (NLP): classification, translation, sentiment analysis, etc.
- Large Language Models (LLM): document question answering, intell. chatbot automation, text generation, etc.
- Other multimodal models: visual answering, image or audio generation (e.g. from text), etc.

As a result, current MLOps practices need to focus on incorporating the (primarily API-driven) integration of external (mostly SaaS or at least hosted) solutions. These SaaS services are great since they are usually easy to use, do not need deployment infrastructure, and can satisfy various compliance and explainability requirements out of the box, as part of the service. The service providers also provide support and consultancy for applying their services, and billing happens based on usage.

However, in order to incorporate external ML solutions into industrial use cases, new processes are needed to facilitate their integration. These face challenges while employing them in CPSoS use cases as the industrial engineering processes are more waterfall-like and the solution architectures prefer closed, on-premises infrastructures. The solution architecture (and hence the corresponding ML Ops processes) need to take into account the following characteristics of SaaS services:

- secure, private, and reliable connections are needed from the CPSoS for production and nonproduction environments separately;
- SaaS products have their own (non-standard) data models, API designs, and specifications;
- SaaS implement breaking changes in their APIs quite often due to their agile delivery models;
- SaaS hence needs continuous testing with automated test suites to validate functionality and fitness;
- together with iterative and agile security and safety verification steps;
- SaaS platforms have internal observability tools that need connectors from CPSoS.

B. Digital Twins

In the Digital Twin concept, there are both physical and virtual representations of the same object or process, and their change in status parameters affect the behavior of each other within a given context. The physical entity and its digital twin are interconnected. A typical scenario is that the parameters of the physical entity get measured, and its virtual software model changes its status to match the physical entity's measured status. The more refined the digital model is, and the more detailed the status-information exchange, the better the digital and physical representation matches. As we can conduct high-speed calculations and predictions with the digital model, we can suggest control commands to the physical entity, which altogether leads to better performance, fewer errors, and safer operations in the physical world [20].

There are various ways to design and operate Digital Twins. One of the current trends in the industry 5.0 concept is to apply the model-based approach in this domain [21]. These, together with the requirements and application categories [9] mentioned in the related work section, substantiate that DT-

related subtasks are necessary to appear in the extended MLOPs workflow and toolchain that endorses CPSoS.

IV. ML Ops for Industry 5.0

A. Engineering Process for Cyber-Physical System of Systems

Standardized process model descriptions for industrial engineering contribute significantly to the effectiveness of engineering complex system of systems. The Automation Engineering Model of the ISO/IEC 81346 standard [23] defines such a process. The Arrowhead Tools Engineering Process (AHT-EP) – introduced in [22] and depicted by Figure 4 – is an extended version of ISO 81346, as it is applicable for dynamic, service-oriented CPSoS. The core design principle of AHT-EP is to harmonize flexibility and adaptability with the robustness inherited from earlier process models, so it can be adapted to various industrial domains from manufacturing to production, from energy grids to logistics.

Just like in DevOps, tools are associated with the steps of the ISO/IEC 81346 standard and of its extension, the AHT-EP. In other words, we can categorize tools that are useful in Functional Design (step 2) or that can be of major help in Deployment and Commissioning (step 4). Besides extending the standard, the practical benefit of using the AHT Engineering Process is that tools can be associated for each of the $n = 1..8$ steps. If we tailor the output of the $step_n$ tool to the input of the $step_{n+1}$ tool, humans can focus on more meaningful tasks than format conversions.

Use-case examples for automatic execution of such toolchain steps are provided by [22]. These process models pose, in general, some requirements on the solution architecture involved: namely that (i) the technology toolchain and solution platform is relatively stable throughout the cycle, (ii) the infrastructure and deployment requirements are established at project start, (iii) operational model can be clearly established at an early stage.

Nevertheless, in order to fit the current reality of AI/ML-supported productization lifecycles and tools, this AHT-EP needs to be matched with the ML Ops toolchain, as well as with Digital Twinning (i.e., creation, operation, synchronization, verification, and validation). The DT models need to be continuously fed production data, and the output of DT models might be reused for training and validating other ML applications.

B. The Olympics Model for MLOps-Coupled CPS Engineering

As the proposed process goes, the whole MLOps lifecycle needs to be augmented with the requirements driving the Digital Twin and Systems Engineering design flow. As described earlier, the challenge is bringing the AHT-EP and other CPSoS engineering standard development processes together with the ML-Dev-Ops cycles of the organization.

In this paper, building on the above-mentioned related works, we propose the extension of the DevOps and MLOps process (as seen in Fig. 3) with two additional aspects: managing the Digital Twin lifecycle and integration of the DevOps aspects with the industrial Systems Engineering process. This newly proposed process model – resembling the five circles of the Olympics – is illustrated by Figure 5.

Furthermore, a CI/CD model, together with an appropriate toolset for CPS applications, is suggested in [24]. The process is illustrated for (Arrowhead-capable) CPSoS in Figure 6, which is especially useful for System of Systems containing resource-constrained devices (e.g., microcontrollers and other equipment without any operating system), edge computing platforms and corporate on-premises or public cloud infrastructure jointly. This diagram also assumes the join venture between various IT and OT groups in an agile delivery model, where all aspects of the CPSoS can be continuously deployed and orchestrated with the same framework: embedded systems, control systems, as well as enterprise applications. Here, the following details need to be considered:

1) The Digital Twin lifecycle: is the first extension of the traditional DevOps model. Either model-based [21] or not, the *creation* of the DT and its continuous *synchronization* is essential. Furthermore, the functional, safety and security verification and validation *(V&V)* of the connected DT (that might be an ML) model has to be an essential part of the workflow.

– *DT creation* is influenced by two things: the system model of the *SysEng cycle* (i.e., mapped with "Procurement & Engineering (3)" of AHT-EP), and the verified and developed software of the *Dev cycle*. The Digital Twin can be created – and re-created – based on these inputs and their changes in time.

– *DT synchronization* is a continuous task, enabled by low-latency communication. The more refined the DT model is (in time-granularity and in functional variables), the better the CPSoS control options are.

– *V&V* stands for Validation and Verification, and it is a distinguished task in ML-coupled CPS engineering. It is responsible for making sure not only functional V&V, but also V&V in terms of security and safety. This is why we dedicated section IV-C to describe the background of this task below. Once the V&V is successful, it results in the MLOps lifecycle to startup the Packaging step on the Dev cycle and the Deployment in SysEng cycle.

2) The SysEng lifecycle: corresponds to well-established Engineering processes, such as ISO 81346 or AHT-EP. As the latter is overstretched (from requirements to training and education), the SysEng cycle in the Olympics model uses its process steps from "Functional Desing (2)" to "Evolution (7)".

– *SysModel* – as in System Modeling – covers the initial steps of AHT-EP, such as "Functions Design (2)" and "Procurement and Engineering (3)". This also feeds the DT Creation task. Depending on the CPSoS and the use-case, many matured system engineering tools are available to support the SysModel phase.

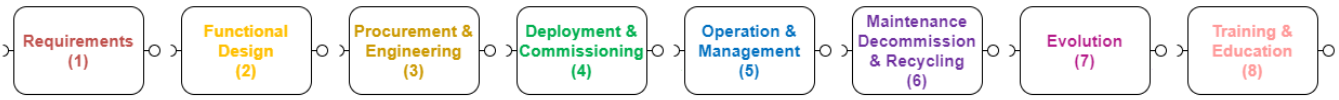

Fig. 4. The graphical overview of the Arrowhead Tools Engineering Process [22]

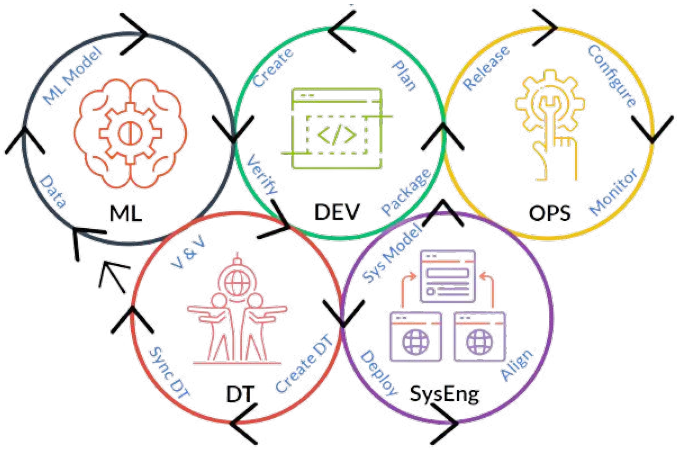

Fig. 5. The Olympics model for MLOps-coupled CPS engineering

– *Deploy* is the same task as "Deployment and Commissioning" as in ISO 81346 or AHT-EP.

– *Align* is responsible for fine-tuning the model after deployment of the DT, and leading to the Ops cycle –, including steps "Operations & Management (5)", "Maintenance, Decommission & Recycling (6)" and "Evolution (7)" of AHT-EP.

C. Validation, Safety, Security

Regarding Industrial application settings, the MLOps process clearly needs to be secured, against attacks targeting the training data, the training process, the model, and the query, as described by [25]. Going into further details, the authors of [26] propose a structured verification at each phase of the ML development process (ML lifecycle) in three dimensions, namely data, code, and model. They argue that the verification of these components at each phase could cover the verification of the ML system as a whole. Still, this proposal misses cross-validation and verification of some non-functional features of ML-integrated CPSoS.

In our view, the validation and verification for CPSoS and Digital Twins must go further and requires the creation of methods and procedures on:

- safety;
- time-criticality;
- responsible usage;
- human acceptance (i.e., through XAI or other approaches),
- integrability;
- decision control allowances.

D. MLOps Engineering Toolchain for Industrial Applications

As described above, based on the requirements set in Section II, design adaptation is required for the "de-facto standard" MLOps solution architecture. The proposed solution of this paper is presented in Figure 7. This takes into account the details presented in the Related Works and considerations made for Digital Twins, ML Ops practices, the involvement of SaaS solutions, and the current engineering process for CPSoS. In this Figure, blue colored components represent the main integration points (i.e. source and destination systems) of the CPSoS; the "observability" components are highlighted with yellow color (i.e. Digital Twin), while the data platform components (green color), the ML Ops CICD (orange) and the ML infrastructure (red) are also depicted in one continuous cycle of data (and model) flow. In this proposed toolchain, the "de-facto" *MLOps* lifecycle is continuously executed on:

- *ML Infrastructure* elements – which also appear in those MLOps models that are extended with the infrastructural view, and refer to a hybrid cloud setup wih resources deployed in the edge or corporate on premises, in public clouds or procured as SaaS.
- *Cyber-Physical Production Systems* elements – that represent Industry4.0 and 5.0 data sources of various levels, including individual CPSs, the Manufacturing Execution System (MES) and various corporate systems.
- *Data Platform* - for ETL: Extract, Transform and Load the collected data arriving from the data sources; then feeding forward into exploration mechanisms, the Digital Twin synchronization mechanisms, and into the continuous and automated ML validation and verification testing.
- *Digital Twins* and their *Monitoring and Telemetry* – for real-time status sync' of DTs and building new ML models based on production data. This may use separate data collectors outside of the Data Platform.
- *AI Gym* – or similar sandbox platforms and environments for exploration and validation; working with a sanitised copy of production data for development purposes.

Here, an additional set of couple of key differences and customisation requirements need to be considered:

1) The sources of data are industrial CPSoS and other B2B integration systems.
2) The corporate data platform must integrate with the Digital Twin solution bi-directional (feed-forward and feedback nature).
3) Edge AI platforms have very limited capabilities compared to cloud platforms, they need specialized deployment automation.

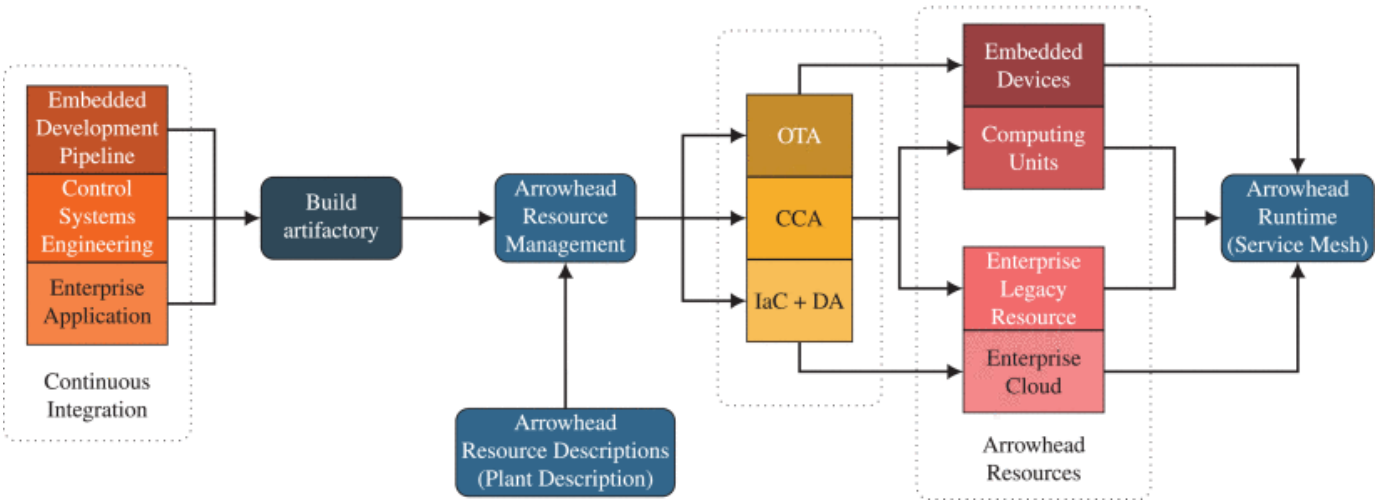

Fig. 6. A DevOps pipeline for Arrowhead-capable CPS – Note: OTA: "Over-the-Air" - CCA: "Continous Configuration Automation" - IaC: "Infrastructure as Code" - DA: "Development Automation" [24]

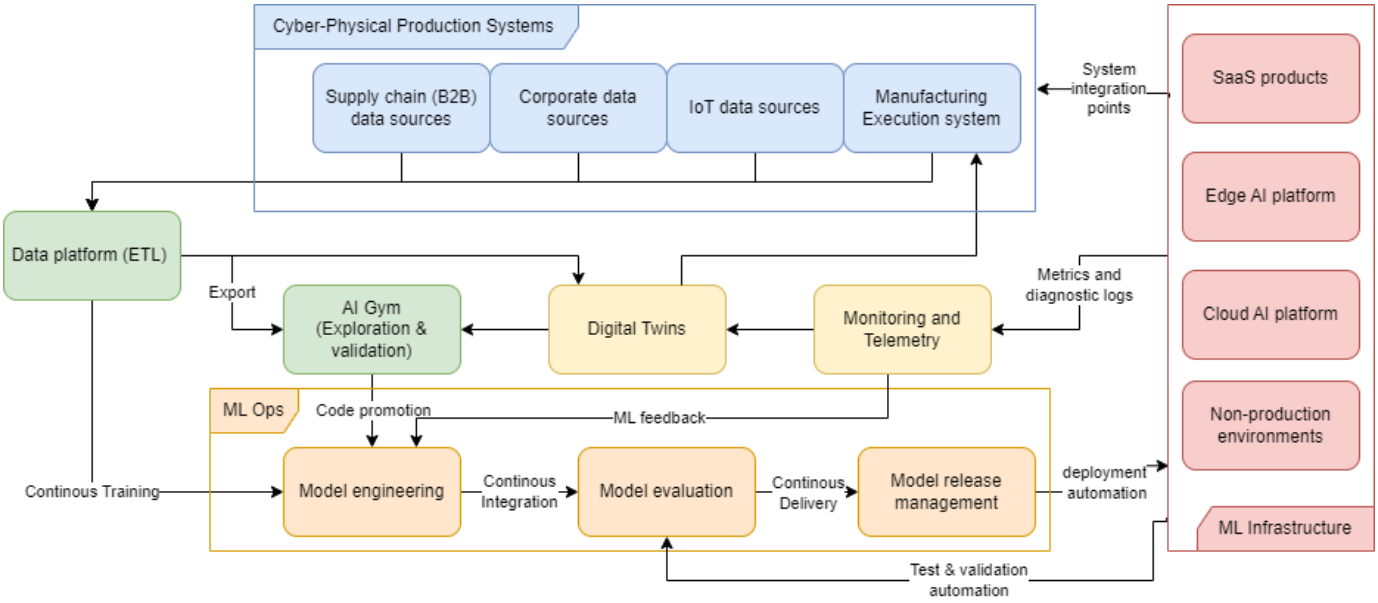

Fig. 7. Reference MLOps Engineering Toolchain for industrial use cases

4) Industrial ML projects require specialized and isolated sandboxes for development.
5) Continuous Training and Continuous Deployment practices are not possible due to the strict waterfall-like engineering standards; a strict promotion process is needed between non-production and production.
6) In-production testing is mostly not feasible (e.g., blue-green testing) for industrial cases due to the CPSoS nature.
7) The test and validation automation stack must include or mock CPSoS upstream services.

These requirements facilitate the concept of "AI gyms" that need to be a non-production sandbox allowing ML developers to work with sanitized production and DT data, while not being able to verify and validate their work end-to-end. Here, ML engineers can execute the initial phases of modelling and implementation, focus on the model serving (and systems integration work) ahead. This AI gym needs to be able to (i) simulate various parts of the CPSoS and DT, (ii) emulate the underlying hybrid infrastructure and (iii) run the nightly V&V automation stack, if it exists.

These requirements also mandate a deployment automation stack that is overseen manually and can deploy ML applications together with the changes in other elements of the CPSoS (hence merging the concepts of Figure 7 with Figure 6). Future work is to bring these together from solution architecture perspective, i.e. bridging the deployment automation stacks of the various domains into one DevOps pipeline.

V. Conclusions

As MLOps techniques get widely applied throughout all ICT domains, their adoption to Industry 4.0 and 5.0 use-cases gets compelling as well. The main reason that industrial production adopt the newest technologies slower than the IT sector lays in the physical nature of the production (i.e., safety), and in the tight optimization criteria of production performance (i.e., long ROI). Besides, there is a push against the industrial players to reduce time-to-market for innovations by utilizing the latest technologies, such as ML in Digital Twins. Due to this push, responsible AI and explainable AI are to be included in the requirement mix. The MLOps techniques have to be extended for industrial usage, where the process models and toolchains take into account these needs.

In our paper, we created two views for MLOps extensions for the industry. One is the Olympics model for MLOps-couples CPS Engineering, which extends the "infinity loop" model of MLOps with tasks related to Digital Twins, and with a cycle of the System Engineering process. Besides, the second model is the MLOps Engineering Toolchain for industrial applications, extending the data engineering viewpoint of MLOps with data sources, infrastructural tasks and also, the Digital Twins and their monitoring and telemetry. These models are planned to be serving as a basis for the EU KDT project AIMS5.0 (Artificial Intelligence in Manufacturing leading to Sustainability and Industry5.0), where 53 partners work together in 20+ industrial use-cases.

Although digital supply chain (DSC) management is not the focus of these scenarios, the concepts described in this paper can and should be extended with the DSC dimension [27]. One of the future works for our study is to extend it toward supply chain management (SCM) utilization. There are various application areas of AI in DSC, as surveyed in [28]. The requirements and challenges set by SCM applications require further extensions of our models presented in this paper.

Acknowledgment

The research leading to these results is funded by the EU KDT-JU organization under grant agreement 101112089, within the project *AIMS5.0* and from the partners' national programs and funding authorities.

References

[1] A. Renda, S. Schwaag Serger, D. Tataj, A. Morlet, D. Isaksson, F. Martins, M. Mir Roca, C. Hidalgo, A. Huang, S. Dixson-Declève, P. Balland, F. Bria, C. Charveriat, K. Dunlop, and E. Giovannini, *Industry 5.0, a transformative vision for Europe: governing systemic transformations towards a sustainable industry*. EC Dir.-General for R.&I., 2021.

[2] P. K. R. Maddikunta, Q.-V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: A survey on enabling technologies and potential applications," *Journal of Industrial Information Integration*, 2022.

[3] D. Kreuzberger, N. Kühl, and S. Hirschl, "Machine learning operations (mlops): Overview, definition, and architecture," 2022.

[4] A. Angelopoulos, E. T. Michailidis, N. Nomikos, P. Trakadas, A. Hatziefremidis, S. Voliotis, and T. Zahariadis, "Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects," *Sensors*, vol. 20, p. 109, 2019.

[5] A. E. Frankó and P. Varga, "A survey on machine learning based smart maintenance and quality control solutions," *Infocommunications Journal*, vol. 13, no. 4, pp. 28–35, 2021.

[6] Infineon, "Aims 5.0 project," https://blogs.nvidia.com/blog/2020/09/03/what-is-mlops/, 09 2023.

[7] M. U. Querejeta, L. Etxeberria, and G. Sagardui, "Towards a devops approach in cyber physical production systems using digital twins," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2020, pp. 205–216.

[8] Y. Jiang, S. Yin, K. Li, H. Luo, and O. Kaynak, "Industrial applications of digital twins," *Philosophical Transactions of the Royal Society A*, vol. 379, no. 2207, p. 20200360, 2021.

[9] Z. Huang, Y. Shen, J. Li, M. Fey, and C. Brecher, "A survey on AI-driven digital twins in industry 4.0: Smart manufacturing and advanced robotics," *Sensors*, 2021.

[10] P. J. Phillips, C. Hahn, P. Fontana, A. Yates, K. K. Greene, D. Broniatowski, and M. A. Przybocki, "Four principles of explainable artificial intelligence," 2021-09-29 04:09:00 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933399

[11] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of Industrial Information Integration*, vol. 6, pp. 1–10, 2017.

[12] A. Bicaku, C. Schmittner, P. Rottmann, M. Tauber, and J. Delsing, "Security safety and organizational standard compliance in cyber physical systems," *Infocommunications Journal*, vol. XI, p. 2, 03 2019.

[13] S. Mittal, M. A. Khan, D. Romero, and T. Wuest, "Smart manufacturing: characteristics, technologies and enabling factors," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 233, no. 5, pp. 1342–1361, 2019.

[14] NVIDIA, "What is mlops?" https://blogs.nvidia.com/blog/2020/09/03/what-is-mlops/, 09 2020.

[15] N. Hewage and D. Meedeniya, "Machine Learning Operations: A Survey on MLOps Tool Support," 2022. [Online]. Available: https://arxiv.org/abs/2202.10169

[16] INNOQ, "Machine learning operation," https://ml-ops.org/content/end-to-end-ml-workflow, 08 2023.

[17] M. Testi, M. Ballabio, E. Frontoni, G. Iannello, S. Moccia, P. Soda, and G. Vessio, "Mlops: A taxonomy and a methodology," *IEEE Access*, vol. 10, pp. 63 606–63 618, 2022.

[18] IBM, "What is etl?" https://www.ibm.com/topics/etl, 09 2023.

[19] T. L. Foundation, "LF AI and Data Foundation Interactive Landscape," https://landscape.lfai.foundation/, 08 2023.

[20] F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," *IEEE Transactions on industrial informatics*, vol. 15, no. 4, pp. 2405–2415, 2018.

[21] M. Balogh, A. Földvári, and P. Varga, "Digital twins in industry 5.0: Challenges in modeling and communication," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–6.

[22] G. Kulcsár, P. Varga, M. S. Tatara, F. Montori, M. A. Inigo, G. Urgese, and P. Azzoni, "Modeling an industrial revolution: How to manage large-scale, complex iot ecosystems?" in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021.

[23] IEC, "Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations – Part 1: Basic rules," Standard IEC 81346-1:2022, March 2022.

[24] C. Hegedűs, P. Varga, and A. Frankó, "A DevOps Approach for Cyber-Physical System-of-Systems Engineering through Arrowhead," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 902–907.

[25] C. Kempka and A. Schaad, "Securing the ml lifecycle," Tech. Rep., 03 2022.

[26] S. R. Kaminwar, J. Goschenhofer, J. Thomas, I. Thon, and B. Bischl, "Structured verification of machine learning models in industrial settings," *Big Data*, vol. 11, no. 3, pp. 181–198, 2023.

[27] D. Kozma and P. Varga, "Supporting digital supply chains by iot frameworks: Collaboration, control, combination," *Infocommunications Journal*, vol. 12, no. 4, pp. 22–32, 2020.

[28] M. Pournader, H. Ghaderi, A. Hassanzadegan, and B. Fahimnia, "Artificial intelligence applications in supply chain management," *International Journal of Production Economics*, vol. 241, p. 108250, 2021.