
The dissertation investigates the potential of integrating advanced communication protocols, cybersecurity measures, and robotics systems in the context of smart manufacturing. The primary objective is to enhance the efficiency and effectiveness of smart factory operations by addressing challenges associated with implementing Digital Twins (DT) in Industry 4.0 environments.

Chapter 1, "Introduction," provides an overview of the research objectives, outlining the significance of DTs in smart manufacturing and the challenges associated with their implementation. This chapter sets the context for the subsequent in-depth investigations into advanced communication protocols, cybersecurity measures, and robotics systems.

Chapter 2, "Streaming Machine Generated Data via the MQTT Sparkplug B Protocol for Smart Factory Operations," explores the implementation of MQTT Sparkplug B as a communication protocol within smart factories. This chapter assesses the advantages of this protocol in terms of speed, flexibility, and lightweight architecture and examines its effectiveness in creating a unified namespace essential for realizing DTs in manufacturing environments.

Chapter 3, "Machine Identity Authentication via Unobservable Fingerprinting Signature: A Functional Data Analysis Approach for MQTT 5.0 Protocol," presents a novel method for authenticating manufacturing machinery. This approach utilizes unique vibration signatures from machine operations, creating a reliable, unforgeable identity marker that significantly boosts cybersecurity in smart manufacturing environments. By employing functional data analysis, the research develops vibration-based Unobservable Fingerprinting Signature (UFS) system, designed
for smooth integration with the MQTT 5.0 protocol. The chapter rigorously evaluates the method's practicality, showing its ability to authenticate machine identities accurately and efficiently, mitigating insider threats and unauthorized interventions. It emphasizes the method's importance in securing the manufacturing process, offering insights into optimizing machine learning models for robust cybersecurity frameworks within Industry 4.0, and suggests its widespread application in industrial IoT, enhancing secure smart manufacturing practices.

Chapter 4, "Advancing SME Manufacturing Efficiency: Integrating Digital Twins and Computer Vision for Dynamic Production Adaptability," delves into the practical application of DT technology within the NVIDIA Omniverse platform, offering a transformative use case for small and medium-sized enterprises (SMEs) in the manufacturing sector. This chapter illustrates how integrating DT and computer vision technologies optimizes material handling in CNC machines, embodying the essence of smart factory operations. It highlights the development and operationalization of a flexible robotic/CNC cell, underpinned by DT, demonstrating how SMEs can achieve unprecedented adaptability and efficiency. The implementation within NVIDIA Omniverse not only serves as a vivid example of DT's potential to streamline manufacturing processes but also provides SMEs with actionable insights and a replicable model to enhance productivity and maintain competitiveness in the rapidly evolving manufacturing landscape.

By conducting an in-depth investigation of these key aspects, this dissertation aims to provide valuable insights into the successful integration of advanced communication protocols, cybersecurity measures, and robotics systems in smart manufacturing. The research contributes to the ongoing development of Industry 4.0 and its impact on the future of manufacturing by addressing the challenges and opportunities associated with implementing DTs and other innovative technologies.
Securing the Future of Smart Manufacturing: Integrating Digital Twins, Cybersecurity, and Advanced Communication in Industry 4.0

by
Pavel Koprov

A dissertation submitted to the Graduate Faculty of North Carolina State University in fulfillment of the requirements for the degree of Doctor of Philosophy

Industrial Engineering

Raleigh, North Carolina

2024

APPROVED BY:

_______________________________  ________________________________
Dr. Binil Starly               Dr. Yuan-Shin Lee
Committee Co-Chair            Committee Co-Chair

_______________________________  ________________________________
Dr. Xiaolei Fang              Dr. Paul Cohen
Committee Co-Chair

Dr. Dan Harris
DEDICATION

To my loving family, whose unwavering support, encouragement, and belief in me have been the foundation upon which I have built my academic pursuits. Your love, sacrifices, and constant presence have given me the strength to continue on this journey.

To my esteemed advisor, who has guided me with their invaluable knowledge, expertise, and mentorship throughout the course of this dissertation. Your patience, understanding, and dedication to my growth have been instrumental in shaping my academic and professional development.

To the professors who have taught, inspired, and challenged me during my time in academia. Your passion for knowledge and commitment to educating the next generation of innovators has profoundly impacted my intellectual curiosity and growth.

And finally, to the entire manufacturing world, which continues to evolve, innovate, and drive our global society forward. This research is dedicated to all those who tirelessly work to improve the processes, technologies, and methodologies that shape our modern world. May the insights gleaned from this dissertation contribute to the betterment of the manufacturing industry, as we collectively strive to create a more efficient, sustainable, and productive future.
BIOGRAPHY

Pavel Koprov is a distinguished industrial engineer and researcher with a strong background in machine learning, robot control, and IIoT for advanced manufacturing. Born in Polyarniy, Murmanskaya oblast, Russia in January 1992, Pavel pursued his academic interests, obtaining his Bachelor's and Master's degrees in Automatic Systems Engineering from Sevastopol State University in 2012 and 2013, respectively.

Before joining NC State, Pavel gained valuable industry experience, working for six years as a leading design engineer and design engineer in the field of advanced manufacturing. His practical expertise, combined with his academic pursuits and leadership positions, has positioned Pavel as a well-rounded expert in the realm of smart manufacturing and industrial engineering.

Pavel's journey in the industry took a significant step forward in the summer of 2023 when he interned at Dow Chemical. This experience further honed his skills in Data Science. Building on this successful collaboration, Pavel is set to return to the Automation group of Dow Chemical R&D in the summer of 2024 as a full-time employee, a testament to his capabilities and the value he brings to the field of smart manufacturing.

Currently a Ph.D. candidate in Industrial Engineering with a focus on Smart Manufacturing at North Carolina State University, Pavel serves as a graduate teaching and research assistant. During his time at NC State, he has been actively involved in research and development projects aimed at connecting machines on the factory floor through a digital thread. Pavel has also played a significant role in creating the DT of the Advanced Manufacturing Lab and has contributed to research efforts centered on developing smart collaborative robots (cobots) using a self-learning framework.
In addition to his academic and research pursuits, Pavel is an engaged leader at NC State, serving as the President of the Society of Manufacturing Engineers Student Chapter and the President of the Industrial and Systems Engineering Graduate Student Association. These roles have allowed him to make a significant impact on the university community and promote collaboration among students and faculty in his field.
ACKNOWLEDGMENTS

First and foremost, I would like to express my deepest gratitude to my advisor, Dr. Binil Starly. His exceptional ability to generate innovative ideas, unwavering belief in me, and dedication to discussing various research directions in smart manufacturing have been invaluable. I am truly grateful for the trust he has placed in me throughout the past three years. Without his guidance and support, this work would not have been possible.

I would also like to extend my appreciation to Dr. Yuan-Shin Lee, under whom I served as a Teaching Assistant and student. His passion for education and commitment to student involvement provided me with the opportunity to work in this team. I am equally grateful to Dr. Paul Cohen for his valuable feedback and to Dr. Dan Harris for introducing me to statistics and offering invaluable guidance throughout my statistical endeavors, including this work. Special thanks go to Dr. Xiaolei Fang, whose assistance in the data analysis of vibration data was instrumental in the development of two of my papers on Unobservable Fingerprinting Signature. His expertise and support were crucial in navigating the complexities of this research area. Additionally, I extend my gratitude to the faculty at NC State, particularly Dr. John-Paul Ore, Dr. Frederick Livingston, Dr. Jingyan Dong, and Dr. Ola Harrysson, for teaching outstanding courses that have been crucial for the completion of this dissertation.

I would like to express my gratitude to the DIME lab members, Akshay, Connie, Thomas, and Aman, for engaging in intellectually stimulating discussions that made my time at the DIME lab both enjoyable and fulfilling. Many thanks to my friends Ian, Satya, Troy, Erik, and Sam for the unforgettable experiences we shared in Raleigh. Finally, I want to acknowledge my peers at ISE GSA and SME, including Nafi, Madi, and Delaney, for their support and camaraderie throughout this journey.
TABLE OF CONTENTS

1.1 Introduction ......................................................................................................................... 1
1.2 Background .......................................................................................................................... 3
1.3 Motivation ............................................................................................................................ 5
1.4 Problem Statement and Research Objectives ...................................................................... 7
1.5 Proposed Work ..................................................................................................................... 8

2.1 Introduction .......................................................................................................................... 13
2.2 Project Goal .......................................................................................................................... 16
2.3 Literature Review ............................................................................................................... 18
2.4 Methods ............................................................................................................................... 21
  2.4.1 System Architecture of Pub/Sub Model within Factory ................................................. 21
  2.4.2 Hardware and Software Setup ....................................................................................... 23
  2.4.3 Pub/Sub Model via MQTT-SpB Specification ............................................................... 24
  2.4.4 Machine Profiles on CESMII SMIP ............................................................................ 27
  2.4.5 Streaming Data to CESMII SMIP Cloud ..................................................................... 28
2.5 Results .................................................................................................................................. 29
  2.5.1 Cloud and Local Factory Monitoring Dashboard .......................................................... 29
  2.5.2 Powering Digital Twins (3D Models) ............................................................................ 30
2.6 Conclusion ........................................................................................................................... 31
2.7 Acknowledgments ............................................................................................................... 33

REFERENCES ............................................................................................................................ 34

3.1 Introduction .......................................................................................................................... 39
3.2 Project Goal and Contributions ............................................................................................ 41
  3.2.1 Overview ....................................................................................................................... 41
  3.2.2 Project Goals ................................................................................................................ 41
  3.2.3 Contributions to Smart Manufacturing ....................................................................... 42
  3.2.4 Implications for Cybersecurity in Industry 4.0 ............................................................. 43
3.3 Literature Review ............................................................................................................... 43
  3.3.1 Advances in Physical Unclonable Functions and Their Application ......................... 43
  3.3.2 Functional Data Analysis ............................................................................................. 46
  3.3.3 Security of the MQTT Protocol ................................................................................... 47
3.4 Methods ............................................................................................................................... 49
  3.4.1 Hardware and Software Setup ...................................................................................... 49
  3.4.2 Password Moves ........................................................................................................ 52
5.2.5 AI-Driven Applications Leveraging Transformer Models ............................. 123
5.3 Conclusion ........................................................................................................ 124
LIST OF TABLES

Table 2.1 Publisher Client pseudocode

Table 2.2 Subscriber (Historian) pseudocode

Table A1 Sensitivity and specificity of tested ML models for every asset
LIST OF FIGURES

Fig. 1.1 Google trends of terms Digital Twin and Industrial Internet of Things from April 2019 to April 2024 (accessed Apr. 1, 2024) .................................................................................................................. 1

Fig. 1.2 Components of Smart Factory framework. Red background contains topics that are supported by current work .......................................................................................................................... 3

Fig. 2.1 Industrial implementation of MQTT SparkPlug™ B protocol ........................................ 22

Fig. 2.2 The architecture of machine data collection from Haas machines ................................ 23

Fig. 2.3 Generic CNC Profile defined within the CESMII SMIP .............................................. 28

Fig. 2.4 Dashboard of key metrics transferred from two CNC machines in real-time .......... 30

Fig. 2.5 Example of DT (c) consuming data published by the physical asset (a) through subscribing to the device DDATA topic (b) .................................................................................................... 31

Fig. 3.1 Enhanced handshake in MQTT 5.0. It is proposed that machines send their UFS through the AUTH packet ..................................................................................................................... 49

Fig. 3.2 Initial (a) and consecutive (b) hardware setup on VF-2 CNC milling machine............ 50

Fig. 3.3 Location of IMU on assets: a) platform of UR robot, b) backplate of Bambu printer .... 51

Fig. 3.4 Password moves for the subject asset types ............................................................... 54

Fig. 3.5 Vibration patterns of UR cobots. Ovals highlight the differences in signals. Black ovals show the difference for UR-10e. Green ovals highlight the difference between 2 similar UR-5e patterns. Purple ovals highlight the difference between the other two similar UR-5e patterns.... 56

Fig. 3.6 Vibration patterns of Prusa 3D printers. Ovals highlight the differences in signals. Each oval circumscribes part of the signal specific to only one printer .......................................................... 56

Fig. 3.7. Vibration patterns of VF-2 CNC machines. Ovals highlight the differences in signals. 56

Fig. 3.8 Acceleration on X axis time series data plotted for UR robots. Grey lines represent collected data, red and blue curves are the shapes of upper and lower mean bounding shapes ... 60

Fig. 3.9 Original and reconstructed curves. Blue is the original curve and orange is the reconstructed curve from FPCS. The upper plot shows the mean curve for training data (UR5e_N). The middle plot shows the random curve of one of the UR5e_W samples .......... 62

Fig. 3.10 Performance metrics of initial FPCA (a, b, c) and OCSVM (d, e, f) models of UR robots. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM ........................................................................ 63
Fig. 3.11 Performance metrics of initial FPCA (a, b) and OCSVM (c, d) models of VF-2 CNC machines. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM................................. 64

Fig. 3.12 Performance metric of initial FPCA (a, b, c) and OCSVM (d, e, f) models of Bambu printers. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM................................. 64

Fig. 3.13 Longitudinal performance of FPCA “old” models: a) VF-2 machines, b) Bambu printers, c) UR robots. X axis – day, Y axis – the normalized reconstruction error..................... 69

Fig. 3.14 Longitudinal performance of FPCA updated models: a) VF-2 machines, b) Bambu printers, c) UR robots. X axis – day, Y axis – the normalized reconstruction error..................... 70

Fig. 3.15 Adaptation to equipment dynamics performance of asset models ....................... 71

Fig. 4.1 ISO 23247 framework applied to our use case.................................................. 98

Fig. 4.2 USD representations of the VF-2 milling machine and UR10e cobot: a) with stage lights and enclosure, b) with VF-2 lights and without enclosure ............................................. 101

Fig. 4.3 Incorporating Isaac Cortex architecture into our robot/CNC cell DT .................. 107

Fig. A2.1 Decision boundaries for OCSVM. Blue circles represent training scores. Red circles represent test scores for target data, and empty circles represent non-target data. The red line is the decision boundary. The test score is a raw scoring function of the samples returned by the OCSVM model................................................................. 127

Fig. A2.2 Decision boundaries for IF. Blue circles represent training scores. Red circles represent test scores for target data, and empty circles represent non-target data. The red line is the decision boundary. The red dashed line is the boundary chosen manually. The test score is a raw scoring function of the samples returned by the IF model................................................................. 128

Fig. A3.1 Performance metric of initial FPCA and OCSVM models of Prusa printers.........129

Fig. A3.2 Performance metric of initial FPCA and OCSVM models of Prusa printers – continued ........................................................................................................... 130
CHAPTER 1 Introduction, Motivation, and Objectives

1.1 Introduction

The White House and the President’s Science & Technology Council have released several legislatures aimed at bringing back manufacturing to the USA and modernizing it through a clean energy paradigm [1]–[5]. This strategy leads to total production automation due to high labor costs in the US. Fortunately, the contemporary level of technology is capable of way more than it was 5 years ago. By 2030, with 500 billion gadgets connected to the Internet and a global machine learning market worth $20.83 billion by 2024, 75.44 billion Internet of Things devices could be in existence by 2025, while the AI market is expected to be valued at over $15 trillion by 2030; consequently, two-thirds of organizations that have effectively utilized Big Data have reportedly experienced a decrease in operational expenses [6]. The paradigms of Digital Twins (DT) and Industrial Internet of Things (IIoT) are steadily gaining popularity and becoming major topics in manufacturing research [7] (Fig. 1.1).

Fig. 1.1 Google trends of terms Digital Twin and Industrial Internet of Things from April 2019 to April 2024 (accessed Apr. 1, 2024)
Implementing and integrating these cutting-edge technologies in production processes is a significant challenge faced by manufacturing facilities [8]. As a result, these facilities are striving to transform their strategies and adopt various planning and control decisions across all levels. This has led to the emergence of the Smart Factory paradigm. As outlined by [9], these systems consist of smart design, machining, monitoring, control, scheduling, and industrial applications. The term "smart" signifies the ability to execute tasks autonomously [10]. Various technologies such as machine learning, artificial intelligence, recommendation systems, deep learning, sensor-based automation, IoT, and big data analytics can be incorporated at any decision-making level to enhance productivity and intelligence.

The widespread adoption of smart manufacturing has heralded the arrival of the fourth phase of industrial production, known as Industry 4.0 [11]. This fourth era, also referred to as the "Fourth Industrial Revolution," "smart manufacturing," "industrial internet," or "integrated industry," is characterized by the production of cyber-physical systems based on the integration of heterogeneous data and knowledge. Industry 4.0 includes an extensive range of technologies and associated concepts, with DTs serving as virtual replicas of physical assets, enhancing connectivity and communication between physical and digital elements. The enablers and features of Industry 4.0 in Smart Factories can be considered key components that facilitate seamless digital connectivity. DTs have a significant impact on areas for advanced manufacturing such as 3D printing, CNC machining, and autonomous robotics (Fig. 1.2). Nonetheless, there is a scarcity of use cases involving DTs for online scheduling, simulation, and machine learning applications in manufacturing area. Although still in the developmental stages, numerous tools for Smart Factory operations are facilitating the progress of Industry 4.0. The IIoT and cybersecurity are critical
components for the successful implementation of DT technology, further contributing to the advancement of Industry 4.0.

Fig. 1.2 Components of Smart Factory framework. Red background contains topics that are supported by current work

1.2 Background

Kortelainen et al.'s article [8] investigates the concept of DT and its application in various industries, focusing on operational and structural types of DTs. The authors analyze the literature and discuss the main use cases for DTs, including condition monitoring, maintenance, physical system life-cycle data management, and decision-making support. They also present examples of adapting the concept of DT to a hypothetical case of a forest machine. The article highlights the lack of detailed information about the implementation of DTs, especially from the software application and system points of view and emphasizes the need for more practical work to demonstrate the viability of the DT concept.

Negri et al.'s article [12] aims to clarify the definition and relevance of DT for the manufacturing sector by analyzing existing research works. The authors find that the main scope of DT was initially to mirror the life of air vehicles with a series of integrated sub-models. Research on DT in manufacturing is an evolution of the ongoing research on Virtual Factories. The paper
highlights the various roles of DT in manufacturing, such as condition-based maintenance, diagnostics, prognostics, and large-scale simulation.

Yi et al.'s article [13] proposes a DT reference model and an application framework for DT-based smart assembly process design based on dynamic generation processes. The authors discuss the components and key enabling technologies for the application framework in detail, providing a theoretical and methodological reference solution for the interaction and fusion between the information and physical worlds of smart assembly. However, the work lacks a real use case, and the results presented are questionable.

Latif and Starly [14], [15] present a DT simulation algorithm for improving the manual assembly process in manufacturing industries that cater to high-mix, low-quantity complex defense systems. The study aims to find the best sequence of manufacturing operations while considering uncertainties such as part arrival, machine breakdowns, data integration, and part obsolescence. By simulating various scenarios, the researchers provide recommendations to enhance the manual assembly workflow, especially in cases of supply chain issues and supplier delays. The case study demonstrates the successful implementation of a DT in a manual, complicated shop-floor problem with uncertainties related to multiple materials, operation sequences, human interactions, and real-world data.

Zhang et al. [16] propose a DT-enhanced dynamic job-shop scheduling method that considers machine availability prediction, disturbance detection, and performance evaluation based on DT data. The case study shows that the proposed method can reduce makespan and total tardiness by 14.5% and 87.1%, respectively, and increase the average utility rate by 14.9%. However, the method may not be suitable for job-shops that cannot provide sufficient data for DT modeling.
Lobbezoo and Kwon [17] explore the application of Reinforcement Learning (RL) in developing a method for replacing high-level task programming in simulated and real-world robotic agents. They create custom representative simulation environments, a combined RL and traditional control methodology, a custom tuning pipeline, and conduct real-world testing, making considerable progress toward their goal.

Xuan et al. [18] use DT technology combined with genetic algorithms to optimize human-robot cooperation in a miniature light bulb assembly production line. The DT helps find the robot's motion trajectory and prevent human-robot conflicts, while the multi-adaptive genetic algorithm calculates optimal ergonomics and creates a worker's movement schedule. This approach optimizes both the robot's movement path and the number of movements performed by the human operator in parallel, saving labor and streamlining the manufacturing process.

In conclusion, most of the current research on DT focuses on high-level architectures, scheduling, condition-based modeling, and workflow prediction. Existing DT applications in robotics often concentrate on individual tasks in isolation from the broader manufacturing processes. However, there is a need to bridge the gap between robotic DTs in the manufacturing space and address skill-based problems in robotic manipulation. My work aims to fill this void by integrating DTs into the manufacturing domain, targeting the challenges of skill-based robotic manipulation. By doing so, the goal is to develop more efficient, adaptive, and robust manufacturing processes that leverage the full potential of DTs and robotic systems in a cohesive and interconnected manner.

1.3 Motivation

The rapid progression of Industry 4.0 has catalyzed the emergence of groundbreaking technologies and methodologies, notably DTs. These virtual models of physical entities or
operations empower superior management and optimization of robotic actions and production processes, eliminating the need for production pauses. This study scrutinizes the capabilities and hurdles of DTs within the ambit of intelligent manufacturing, emphasizing obstacles like cybersecurity and the necessity for novel communication protocols.

DTs markedly advance manufacturing by simulating robotic and production operations in real-time, circumventing disruptions to ongoing output. The fusion of machine learning with DTs facilitates forecasting part quality and renders incessant feedback on machinery performance. Such a synthesis of the tangible and virtual realms augments planning, learning algorithms, and reinforcement learning, thus elevating manufacturing efficacy.

Conventional industrial frameworks and protocols, such as OPC UA, are tailored for deterministic and consistent manufacturing environments, with a bias towards mass production. Nevertheless, the advent of the IIoT and the demand for adaptable manufacturing setups have propelled the creation of alternative protocols like MQTT. These new protocols, especially when amalgamated with Sparkplug B specifications, provide expedited and streamlined means for enacting a unified namespace, pivotal for DTs' efficacious deployment.

In the realm of smart factories and interconnected DTs, safeguarding the security and integrity of these systems emerges as paramount. Implementing cybersecurity strategies is imperative to shield the data exchanged among machinery and authenticate machines akin to biometric verification of human workers. This is crucial for upholding integrity within manufacturing networks and mitigating the risks associated with unauthorized human interference.

The employment of DTs in robotics presents a considerable opportunity to refine machine-to-machine (M2M) communication and furnish contemporaneous insights into the status of manufacturing cells. Access to verifiable data enables robots to operate with heightened
independence and tailor their movements based on the associated DT's condition, thereby enhancing manufacturing processes' efficiency and effectiveness.

DTs harbor the potential to transform smart factory operations by facilitating improved planning and control over manufacturing activities and augmenting robotics' performance within these ecosystems. Nonetheless, challenges such as the requirement for fresh communication protocols and the escalating significance of cybersecurity must be tackled. This dissertation ventures into these challenges, aiming to illuminate the benefits of DTs' incorporation into contemporary manufacturing settings. Through dissecting the synergy between planning, machine learning, and simulation in DTs' milieu, this research endeavors to furnish insights into Industry 4.0's evolution and its implications for the manufacturing sector's future..

1.4 Problem Statement and Research Objectives

The problem statement for this dissertation is: To investigate the potential of DTs in smart manufacturing and identify the challenges associated with their implementation in order to improve planning, machine learning, and reinforcement learning within the Industry 4.0 framework. To achieve this, the dissertation will delve into the following key areas:

1. Analyzing existing industrial communication protocols and architectures, such as OPC UA, and identifying their limitations in the context of DTs. Subsequently, exploring the potential of newer protocols like MQTT, combined with specifications like Sparkplug B, to facilitate the development of a unified namespace essential for DT realization.

2. Investigating the growing importance of cybersecurity in smart factories and DTs, focusing on the development and implementation of robust security measures that protect sensitive information and authenticate machinery, akin to biometric authentication for human workers.
3. Assessing the role of DTs in smart manufacturing, particularly in planning robotic movements and manufacturing processes, and examining how machine learning techniques can be integrated to predict part quality and provide continuous feedback on machinery operations.

4. Examining the potential benefits of incorporating DTs in robotics, particularly in improving M2M communication and enabling autonomous trajectory planning based on the state of the DT, ultimately leading to more efficient manufacturing processes.

By investigating these key aspects, this research aims to contribute valuable insights into the potential of DTs in smart manufacturing and provide a comprehensive understanding of the challenges and opportunities that lie ahead in the ongoing development of Industry 4.0.

1.5 Proposed Work

The proposed work for this dissertation will involve an in-depth investigation of three key areas that are essential for the successful implementation of DTs in smart manufacturing:

1. Implementations of MQTT Sparkplug B for Smart Factory Operations: This section will focus on exploring the potential of MQTT Sparkplug B as a communication protocol within smart factories, examining its advantages in terms of speed, flexibility, and lightweight architecture. The research will assess how this protocol can be effectively utilized in creating a unified namespace, which is vital for realizing DTs in the manufacturing environment.

2. Unobservable Fingerprinting Signature: To address the growing importance of cybersecurity, this section will investigate the development and implementation of an unobservable fingerprinting system for authenticating manufacturing machines. The research will analyze the feasibility and the effectiveness of such a system in maintaining
the integrity of manufacturing networks and preventing unauthorized human intervention for manufacturing machinery.

3. A Study on the Integration of DT for Optimizing Material Handling in CNC Machines within Smart Factory Operations Paradigm: In this section, the research will investigate the effectiveness of DT technology in enhancing material handling within CNC machine operations. By developing and operationalizing a flexible robotic/CNC cell enhanced with DT, the research seeks to demonstrate how such integration can lead to unparalleled adaptability and efficiency in smart factory settings, effectively addressing current limitations in robotic material handling and setting a precedent for future innovations in manufacturing automation.

By conducting a thorough examination of these areas, the proposed work aims to provide valuable insights into the successful integration of DT in smart manufacturing, addressing the challenges associated with their implementation, and contributing to the ongoing development of Industry 4.0.
REFERENCES


CHAPTER 2
Streaming Machine Generated Data via the MQTT Sparkplug B Protocol for Smart Factory Operations


2.1 Introduction

The IIoT can be described as an interconnection of various sensors, actuators, devices, computers, and machines that communicate, share data, and collaborate [1]. Data is envisioned to make physical machine assets on the production floor intelligent and self-aware, leading to the realization of Smart Factories. Factories that leverage data as an asset through flexible communication between machine assets on the floor and higher order information technology (IT) systems enable the factory to be more agile and responsive to production needs. Machine assets on the production floor can send a prodigious amount of data that can be used for many useful applications from machine monitoring, continuous control, real-time visibility, and machine-machine coordination. IIoT enables the implementation of artificial intelligence (AI) based solutions on machine assets, mobile robots, inspection cameras, material handling robots, etc. [2]. IIoT enables Smart manufacturing and is bolstered by several other technologies such as 5G, RFID (radio frequency identification), cloud and distributed computing, and many others. IIoT enabled machine asset devices conventionally do not have enough computing power [3] and must often share the data to other devices with a specific purpose such as Supervisory Control and Data Acquisition (SCADA), Historians, or Analytical systems for Machine Learning (ML) application. The machine assets must have a high data transfer rate with very low overhead. It is easy to imagine
how congested the network can be if the factory floor that consists of thousands of devices begins transmitting data from the Operational Technology (OT) side of the factory over to the Information Technology (IT) systems that power the factory floor enterprise operations.

Conventional methods of industrial communication such as OPC-UA (Object Linking and Embedding for Process Control - Unified Architecture) mostly use a poll/response approach, which may not always be reliable, particularly in scenarios when poor network connectivity through wireless connections and a non-deterministic number of device assets come on and off the network [4]. On the other hand, publish/subscribe (pub/sub) type messaging architecture can alleviate the concerns of a poll-response approach by decentralizing data flow. In MQTT, every machine asset can talk to any other machine asset within the factory floor network via a broker. Recently, the OPC Foundation has released a pub/sub model specification to implement the same data structure through other application layer protocols such as Advanced Message Queuing Protocol (AMQP) or Message Queuing Telemetry Transport (MQTT) [5]. AMQP is heavier and more information rich than MQTT, with benefits and drawbacks (AMQP has its specification and can send bulk messages of indefinite size, while the overhead of a message is much greater) [6]. MQTT was designed for industrial devices with very small computing capabilities and inconsistent network connections. It allows a theoretically indefinite number of devices to exchange information without having a stable connection.

In addition, MQTT consumes traffic only when needed (Report-by-Exception) and does require only regular pinging (default is once per minute). A typical MQTT network includes at least two nodes: a client and a broker. A broker is a de facto server whose role is to retrieve messages published by clients, store for a short time, queue and forward them to the clients who are subscribed to the specific topics. The header of the MQTT message is only 2 bytes.
enabled by MQTT utilizes the pub/sub architecture that secures devices from accessing through network ports. Any authenticated device can subscribe and publish to a topic. Topics themselves maintain a hierarchy that organizes data payload under a hierarchical tree structure. Due to the pub/sub patterns of communications, smarter manufacturing operational services can be delivered over the cloud, enabling more effective management of manufacturing resources for shop floor management. Manufacturing Execution Systems or Manufacturing Operations Management, as defined by the ISA-95 standards, enable its users to track asset utilization, product recipe, statistical process control with data synchronized from the plant floor, through business systems to the executive management. The pub/sub pattern enables a unified namespace of operations that connects various disparate IT systems and OT systems, thereby easing the path to interoperability concerns while maintaining distinct separation of concerns between each IT system.

The MQTT protocol however does not define a standard for how the body of the message is structured, the type of meta-data to be transferred, nor does it define the topic level hierarchy that delineates the organization of data. A recently released version of the MQTT Sparkplug B (SpB) specification addresses some of these concerns, particularly amenable IIoT-based operations [7]. In comparison, the OPC-UA pub/sub model has a much more complicated specification of the message and topics structure than the SpB (on average 25 times heavier), as it is still a client/server specification legacy [5], [8]. Since the memory overhead on OPC-UA is quite a bit higher than MQTT, the power consumption on the edge device is consequently higher. In addition, OPC-UA is open only for the members of the OPC foundation. Combined with industry communication standards such as MTConnect, MQTT SpB can enable the smoother transition and implementation of IIoT within the factory flow without a restrictive licensing model. Once the architecture is laid out in the factory, this data can be permitted to flow out of the factory floor to power cloud-based
applications. These cloud-based apps can be extremely useful to small and medium-scale manufacturers who can rapidly scale the implementation of Smart Manufacturing applications through profile reuse and synergies in laying down a common platform to integrate various apps through standard interfaces.

In collaboration with industrial partners, the Clean Energy Smart Manufacturing Innovation Institute (CESMII) has created the Smart Manufacturing Innovation Platform (SMIP) to enable frictionless movement of information - raw and contextualized data - between real-time operations, people, and the systems that create value across manufacturing processes. The Smart Manufacturing Innovation Platform is an interoperability solution to deliver Industrial 'Plug and Play' applicability to discrete, hybrid, and process-oriented industries. The platform provides secure connectivity to the manufacturer's equipment and processes and adds valuable context so that applications can access information intelligently and through automated mechanisms.

The key technology in the platform is the concept of Profiles, that CESMII is creating to contextually describe sensors, equipment, and processes and generate semantics for data, showing how variables relate to each other. Combining these new concepts in context will provide the ability to define new systems without the need for extensive middleware configuration or infrastructure maintenance and management [9]. The SMIP is a collection of technologies for simplifying access to manufacturing data by normalizing across protocols, enforcing a reusable object model, and guaranteeing an interface contract for application development.

2.2 Project Goal

The main goal of this project is to demonstrate the ability to stream data from machine assets in a unified namespace, particularly when hundreds of machine assets are connected on a network within a digital factory. This work showcases how the MQTT Sparkplug™ B
specification can enable a unified namespace that allows IT/OT technology integration while still enabling interoperability, transparency, and operations security. Real-time data streaming from the machine is stored in local databases and then streamed to the CESMII SMIP, a cloud-based solution that can plug into an extensible collection of apps. The two objectives of this project are as follows:

- The addition of low-cost systems-on-chip devices, such as the Raspberry PI device, acts as an edge node that publishes data reported by the computer numerical control (CNC) unit. The objective is to demonstrate a system architecture that connects machine assets to a factory-wide network of connected machine assets while utilizing available standards such as the MTConnect protocol to structure data obtained from CNC machines semantically.

- Demonstrate how data is streamed locally to data historians directly connected to the factory network and utilize available protocols to stream data to the cloud. We have showcased this project via a local data dashboard that updates its values based on streaming data from the asset. The second scenario demonstrates how data is streamed to the cloud platform for verification and analysis. As data is streamed to the cloud, a semantic layer maps data from the asset (CNC machines) to specific machine profiles based on the MTConnect standard.

This project aims to study the use of new information architecture to ease the integration of IT/OT technologies for Industry 4.0 initiatives. As data is more prevalent and AI/ML applications run on the cloud, this enables scenarios where ML models directly update models embedded within the machine assets on the factory floor. In such cases these machine assets must be in constant communication with cloud-based systems for analytics and intelligent predictive control. Current Factory floor information architectures do not necessarily ease the communication from assets on the factory floor to cloud-based systems.


2.3 Literature Review

Most modern manufacturing processes follow the Reference Model for Computer Integrated Manufacturing (CIM), also known as the "Purdue model" [1]. This framework was proposed in the early 90s and has been de-facto a standard for IT/OT systems implemented for the CIM and led to the development of the ISA-95 standard [2]. The IIoT architecture does not fit this model, especially with Big Data and ML applications. The Purdue model prescribes five layers that separate OT from IT. Levels from 0 to 3 are located on the factory floor and are not connected to the internet. The demilitarized zone, or level 3.5, performs the cybersecurity function and air-gaps the OT from IT. Enterprise levels (4-5) are retrieving only siloed data and cannot connect directly to assets on the factory floor. A five-layered model limits data flow in the context of Smart Manufacturing and specifically in IT/OT integration in an Industrial IoT setting. For example, machine learning models are constantly being updated in the cloud. Device assets on the factory floor would need to access the most recently updated model. Simultaneously, device assets may also need to share specific data generated during operations to update the ML model. The Purdue reference model also does not allow quick equipment addition and operation. This model does not fit the IIoT paradigm since device assets on the shop floor will need to access cloud-level resources. MQTT SpB can be applied to the existing Purdue model and allow access to the data from the IT level and send additional data from ML predictive systems to the OT level.

One well-known way of accessing the data of metal cutting machine tools is via MTConnect. It is a (read-only) royalty-free communication protocol that uses XML and HTTP to request and deliver data from MTConnect-enabled devices [3]. The benefit of this protocol is that it does not require any proprietary software or deep knowledge to access the information from the equipment. One needs to open the browser, type the IP address and the port of the polled asset,
followed by one of the four possible requests: probe, current, sample, or asset. The biggest drawback is that someone needs to create MTConnect Agent and Adapters, which most likely will need to be performed by the original equipment manufacturers (OEM). Ben Edrington et al. [4] implemented the machine monitoring system based on MTConnect and DMG MORI SEIKI assets. Their case utilizes Mori Net and Messenger software developed by DMG MORI and uses the MTConnect protocol. Unfortunately, not all equipment has built-in MTConnect agents, and even those with it might not give all the information needed (Haas MTConnect [5]).

Object Linking and Embedding for Process Control - Unified Architecture (OPC-UA) is a M2M protocol that the OPC foundation designed specifically for industrial applications [6], [7]. Unlike MQTT, OPC-UA uses server/client architecture to poll the client to get the data [8]. Every device type has its proprietary specification that must be followed to work correctly with the OPC-UA server. Classic OT/IT infrastructure includes various devices connected to the OPC-UA servers that communicate with IT structures. All OT participants can also communicate through OPC-UA servers [7]. The data types that can be transferred through those protocols are also predefined by specifications and must completely correspond to the ISA-95 standard [9]. It was shown that there is an issue when one is trying to communicate between different OPC-UA servers or even non-OPC servers [10]. There are several attempts to simplify the use of UA without specific proprietary software [11], [12], but they require substantially more computational power than the MQTT protocol.

Due to the specific needs of the IIoT architecture, the Eclipse foundation developed a special specification called SparkPlug™ [13]. This document specifies the structure of topics, message payload and communication parameters. The generic topic looks as follows:

```
namespace/group_id/meassage_type/edge_node_id/[device_id]
```
A namespace is either "spAv1.0" or "spBv1.0", depending on which specification version is implemented. Group_id can be any UTF-8 alphanumeric string. Message_type indicates how to handle the message payload. Below are listed possible message types:

- **NBIRTH** – Birth Certificate for MQTT Edge of Nodes
- **NDEATH** – Death certificate for MQTT EoN.
- **DBIRTH** – Birth certificate for Devices.
- **DDEATH** – Death certificate for Devices.
- **NDATA** – Node data message.
- **DDATA** – Device data message.
- **NCMD** – Node command message.
- **DCMD** – Device command message.
- **STATE** – Critical application state message.

Some of the devices available at the production floor exploit proprietary protocols or even send analog signals. This necessitates the need for EoN (edge of nodes) – devices that convert proprietary protocol data and analog signals to MQTT Sparkplug data type. Legacy machines that do not communicate through modern protocols can be enabled using EoN devices. On the other hand, those devices labeled as Sparkplug-enabled can publish directly to the device_id topic. SpB specification is critical for IIoT as it defines standardized topic namespace and payload definition. It enables auto-discovery of devices and continuous session awareness. New devices will be easy to find in the network, and their payload structure is deterministic.
2.4 Methods

2.4.1 System Architecture of Pub/Sub Model within Factory

A high-level system diagram demonstrating the concept of pub/sub system architecture is shown in Fig. 2.1. Various machine assets on the shop floor can publish data to an MQTT broker via a topic hierarchy specified by the SpB specification. Different subscriber node types listening to specific topic namespaces pick up the messages and process them as needed. For example, a subscriber listening to messages published by Node N1 is processed and inserted into a plant historian for storage and archival. In another example, subscriber Node S3 might receive a notification that the robot has stopped operation due to a malfunction. Once data enters a historian, this data can be distributed to other client applications, such as visualization dashboards, performing data analysis, etc. The subscriber nodes themselves are not directly communicating with the publisher nodes. The communication happens only through the MQTT Broker topic channels. If industry standards are available, such as the MTConnect standard for CNC machines, this standard can structure the data sent by the publisher. Devices that might be part of a production cell can individually communicate with the broker on specific topics or collectively communicate to the MQTT broker via a production cell-specific topic channel. It is also noted that in the recent MQTT SparkPlug™ B version, subscriber nodes can also publish to specific topic channels at the MQTT broker for system state information (hence double-sided arrows from subscriber nodes in Fig. 2.1).
This unified namespace architecture ensures that machine assets do not need to communicate with higher-order information systems (enterprise resource planning, content management system) through specified controlled layers. Rather a unified namespace is established that allows decentralized machine-machine or machine-cloud communication architecture without the need for centralized nodes that force communication between various levels. MQTT SpB IIoT architecture allows adding any number of new devices to the nodes and any number of nodes to the existing system. It needs only a table from DB to be created before Historian starts to make records for this device or node. Such an approach enables the vast majority of opportunities for Industry 4.0 technologies to be implemented on a production floor.

Fig. 2.1 Industrial implementation of MQTT SparkPlug™ B protocol
2.4.2 Hardware and Software Setup

In this study, four Haas CNC machines were used (2 Haas VF-2 and 2 Haas ST-10), each with the New Generation Control™ (NGC): VF-2 operates on software version 100.19.000.1402, ST-10 runs on software version 100.20.000.1011. There are three possible ways for machine data collection: HaasConnect™, MTConnect, and MDC - Ethernet Q Commands [5]. MDC - Ethernet Q Commands (Q-codes) use either Ethernet or wireless connection to be established. An operator must first establish a telnet connection with a specified IP address and port in this mode. After this procedure, one can send a specific Q-code, and the NGC will return the tag and the value as a text string. This mode was selected to get the data from the CNC machines. Relying on the information retrieved by the Q-codes provided far more data than the in-built MTConnect agent running within the machines. The machine assets, brokers, and subscribers were connected on a virtual private network. These machines were not connected to the broader university-wide infrastructure due to the insecure Telnet protocol. A high-level system architecture is depicted in Fig. 2.2.

Fig. 2.2 The architecture of machine data collection from Haas machines

Each machine asset was connected via Ethernet to a Raspberry PI 4B (RPI) that runs an MQTT Publisher node. Arrows between RPI and CNC machines represent 2-way communication between EoN and the asset. RPIs are connected to the local area network (LAN) through a wireless
connection. LAN makes sure that no one can externally access the network, and Ethernet connection assures that only one device is connected to the CNC. Every RPI contains a 'publisher' daemon that starts whenever the RPI is powered on. Topics and data are structured following the SpB specification v2.2 [13]. MQTT broker is installed on another RPI within the network that is running 24/7. The Historian continuously collects data from the assets and stores them in a PostgreSQL database (DB). Dashboard reads the data from the DB through the REST server. The REST interface provides a middleware layer to collect data requested by client applications (browsers, dashboards, etc.). Important to note that any client in MQTT network is required to know the URI (uniform resource identifier) of the broker. This can either be an IP address or an URL. The amount of devices connected to the network is limited by the network setup. In our prototype setup, the network could connect up to 253 devices in our subnet and 255 devices for the next 254 subnets (more than 65K devices). This can however be further scaled by network address translation (NAT).

The Haas machines’ Q-codes list contains thousands of various parameters and macro variables [14]. Some of these parameters are generic, and some are specific to the model of the CNC machine. Q-codes that retrieved specific CNC machines' timestamps, status/mode coordinates, cutting conditions, and vibration information were utilized for this study. There is also a limit to the number of Q-codes sent through a Telnet protocol before they are read.

2.4.3 Pub/Sub Model via MQTT-SpB Specification

Publisher code was written in Python, including a paho-mqtt library. Configuration files contain the CNC machine's IP address (Ethernet), the IP address of the MQTT broker (for wireless transfer), and the client's name. The CNC IP address is needed for RPI to send Q-codes, and the broker’s IP address is needed to publish. A list of broker IP addresses can contain many values to
supply sustainability of the system. It allows changing the CNC machine and broker addresses without interrupting the main code. The publisher runs in an infinite loop, polling the list of Q-codes as necessary. Data is published to the broker only if there are changes in any of the machine parameters that must be reported. Publisher pseudocode is depicted in Table 2.1.

Table 2.1 Publisher Client pseudocode

```plaintext
Publisher Client pseudocode

read connection parameters from "Pub_config.txt"
read the list of Q-codes from "DB Table columns.csv"
set LWT "OFFLINE" message to NDEATH topic
connect to the MQTT broker
if connection established:
    publish to the topic NBIRTH
    publish to the topic NDATA
else:
    reconnect
if telnet connection is available:
    publish to the topic DBIRTH
    set "running" flag up
else:
    reconnect
while True:
    if STATE topic contains "ONLINE":
        send Q-codes to NGC
        parse data
        if "running" flag is up:
            publish parsed data to the broker
        else:
            publish previous data with flag "STALE"
            set "running" flag down
        publish to the DDEATH topic
```

The following mode of operation is followed: CNC machine does not send data after it is turned on or before it is turned off. The RPI also boots faster than the CNC machine. It publishes node birth certificate and pings telnet port; after receiving the first non-empty response, it is
converted to a start-up message, RPI publishes a device birth certificate and sets a flag of running CNC machine; if telnet connection fails or there are any other reasons RPI loses connectivity with CNC machine, it publishes last known data with flag 'STALE' and device death certificate; when the machine is powered-off RPI also turns down and is not able to publish anything to a broker. It makes the Last Will and Testament message (LWT) published to a node death certificate topic. Most edge devices run continuously and do not need to be powered on/off frequently.

Table 2.2 Subscriber (Historian) pseudocode

---

**Subscriber Client pseudocode**

```plaintext
read connection parameters from "Sub_config.txt"
connect to the database
set LWT message "OFFLINE" to STATE topic
connect to the MQTT broker
publish message "ONLINE" to STATE topic
subscribe to all device and node topics
while True:
    if a new message in any topic:
        print message "Received message in «topic»"
        if node or device name is not in the list of DB tables:
            print("Incorrect topic name")
        else if message is from NBIRTH or DBIRTH:
            make a record in DB that node or device is powered on
        else if message is from topic NDATA or DDATA:
            make a record in DB with node or device data
        else if message is from topic NDEATH or DDEATH:
            make a record in DB that node or device is powered off
```

The main subscriber associated with the Historian uses configuration files to connect to the DB. When the historian code starts first, it publishes 'ready' to the STATE topic after connecting to the DB. It is used by the publishers subscribed to this topic to begin publishing. On the other hand, Historian is also subscribed to birth/death and data topics. The topics' names are compared to the tables available in DB, and if it matches one of the tables, the payload is stored to the DB.
Historian also reads the birth and death certificates and forms respective rows recorded to the DB. Timestamp from Historian is used as a unified source of time. "Keep-alive" time is set for every publisher before connection. MQTT uses a 1.5 times period to reconnect the client. If the client does not respond within this period broker disconnect client and publishes the LWT message. The Subscriber client pseudocode is depicted in Table 2.

The unified namespace decentralized architecture enables the seamless addition of new device assets to the machine or any number of machine assets on the production floor. The pub/sub model also allows easier integration of the IT/OT layers in future factories.

2.4.4 Machine Profiles on CESMII SMIP

Machine profiles provide a semantic taxonomy of tags that help define the characteristic features of physical machine assets. These profiles enable a unified format of type definitions that multiple users can reuse. For example, an original equipment manufacturer (OEM) sells a piece of equipment and includes a Smart Manufacturing Platform profile (SM Profile) that describes the characteristics of the equipment and the run-time data available within it. This SM Profile, or Type definition, can be used to build information systems as features for a machine learning algorithm or to communicate energy consumption information to potential customers [15]. A profile is a generic model of a machine that contains all the working components of the device. Fig. 2.3 gives a sample profile of a CNC machine. As shown in Fig. 2.3, any equipment will have a common set of base components and attributes. This will be true for all devices of the same type used worldwide. Thus, creating a generic profile enables manufacturers to build their equipment type based on a generic model instead of building from scratch, making the process simpler and easier to adopt. The concept of the parent-child relationship also exists within the idea of Machine Profiles.
Fig. 2.3 Generic CNC Profile defined within the CESMII SMIP

2.4.5 Streaming Data to CESMII SMIP Cloud

To facilitate data streaming from the machine asset to the CESMII SMIP Cloud, an Edge Gateway is installed at the facility to facilitate secure high-speed ingress of data into the SMIP. The Gateway (also known as the SM Edge, SM Edge Gateway, or simply the Connector) connects to multiple plant floor (or more genetically OT) data sources to securely transmit data to the core Platform. The Gateway uses an extensible approach to protocol adaptation using Connector Adapters. Connectors can be used to adapt a variety of data sources to the Gateway, which provides store-and-forward and secure data transmission. Though connectors are available for historians such as Wonderware [16] and OSI [17], CESMII SMIP can also accept data directly from MQTT topics through GraphQL. The machine data collected by the edge nodes is written into a PostgreSQL database as time-series records. These records can now be accessed for multiple purposes. Dashboards running locally access the database for live data plotting.

The data is also accessed through Python scripts running locally to utilize GraphQL to write the incoming values to the corresponding tag IDs on SMIP. The process involves a call to retrieve all tag IDs and the related variable names. The names are then matched to the column
names/keys in the Python dictionary pulled from the DB. All tags with non-null values in the table are written as records to SMIP using GraphQL command run from within the Python script. The records update occurs as and when the records are written to the DB, thus reducing delay.

2.5 Results

2.5.1 Cloud and Local Factory Monitoring Dashboard

The purpose of interconnectedness on the factory floor is to make processes more efficient and inform critical decision-making based on key metrics from the process. The best way to visualize processes in real-time is to use dashboards. The largest advantages of using MQTT SpB are the following:

- Disconnection from the main database and restricted access.
- The broker can have multiple subscribers.

Q-codes from Haas NGC support the requirement of most of the parameters that are needed to implement a local factory SCADA system. MQTT's capability to seamlessly add new assets makes it a perfect fit for the Industry 4.0 IIoT. The factory network traffic is not clogged with useless poll/response requests, and any data can be transferred starting from a byte and ending with video files. Dashboards have a minimum latency, retrieve real-time data directly from the MQTT broker, and access historical data from the REST server. In this application, the same data that the CESMII SMIP is subscribing to is also subscribed to by a dashboard application. A sample dashboard is shown in Fig. 2.4.
2.5.2 Powering Digital Twins (3D Models)

DTs [18] can get the information update from the Historian and supply enough data to keep up to date with the physical asset. Haas NGC Q-codes yield enough data to make a visual DT of the CNC machine, implemented within an Autodesk Fusion 360 CAD/CAM environment. In this approach, data published by RPI from one of the VF-2 machines (Fig. 2.5) was utilized to demonstrate the DT of the machine within a CAD/CAM package. We have written Python scripts using Autodesk Fusion 360 API and paho-mqtt library. A 3D model of the Haas VF-2 was downloaded and adapted to reflect the actual machine asset. The plugin script is executed, which enables the Fusion 360-MQTT client to subscribe to the DDATA topic of VF-2 machine and performs movements in 3D space identical to movements of the physical asset. The DT uses the same data source as the Historian and the Dashboard, showing a good example of the unified namespace since it is subscribed to the same topic channels as the Historian and the Dashboard.
2.6 Conclusion

This project demonstrates the application of the MQTT SpB specification to stream data from machine assets on a shop floor through a publish/subscribe model to clients that can be situated both within and outside the factory. This type of communication architecture collapses the Purdue Model by removing structured layers to enable a more node-to-node communication of assets. It allows interoperability between various machine assets and stronger IT/OT networks integration to boost factory-floor visibility from the enterprise level down to the machine asset. The use of profiles within cloud platforms can enable the direct exchange of profiles by small and medium scale manufacturers who can leverage the semantic definition of various machine assets for faster integration of data from the factory floor to a wider expanse of manufacturing apps that can deliver smart manufacturing services and enable smart factories.

This work demonstrated how the MQTT SpB works with Haas CNC machines. Work is still required to translate machine specific codes to gather data and have it transported to subscriber endpoint. This means an information model is required to enable interoperability between various device assets and machine vendors. While information models like MTConnect exists for CNC machines, not all machine types and their associated assets have means to standardize information
coding to enable interoperability. This model required manual selection of parameters and their Q-codes. It can be easily seen that every other vendor has its own proprietary way of accessing the machine data and protocols being used. Other assets will require other approaches to perform data collection.

Lightweight MQTT protocol with SpB specification surpasses OPC-UA and MTConnect protocols in reliability, scalability and the fraction of the useful network traffic consumption. Nevertheless, the absence of wide implementation of this specification in IIoT impedes the development of the plug and play solutions. MTConnect and OPC foundation have been working on finding the optimal solution for the pub/sub IIoT model [19], [20]. Some software solution to use MTConnect and the MQTT protocol also exist on the market [21]. We expect that in the future a companion spec for MTConnect with MQTT is required for further enhancing the use IIoT in factories that have CNC metal cutting machines.

The implementation of our approach can be used in retrofitting of the equipment opposing the work of Etz et al. [22]. The future work orients toward increasing the nomenclature of the equipment type and vendors: CNC machines, robots, conveyor stations, sensor suites, 3D printers, autonomous guided vehicles that are typically used in a production environment. Existing IT systems do not have functionality of direct access to the MQTT broker, thus it has to retrieve the data from DB, which violates the idea of the unified namespace. Future work in this direction is needed to ensure IT software vendors have the ability to communicate (subscribe) directly with the MQTT broker. Sparkplug B has only been released in 2019 and no further revisions are available now. We expect that as adoption and industry specific use cases arise, more revisions and additions will be made to be more applicable in industrial settings.
2.7 Acknowledgments

The work conducted in this project was performed with partial support from CESMII – Clean Energy Smart Manufacturing Innovation Institute through its regional smart manufacturing innovation center funding program.
REFERENCES


081221A837470CF&originRegion=us-east-1&originCreation=20220305194621 (accessed Mar. 05, 2022).


CHAPTER 3

Machine Identity Authentication via Unobservable Fingerprinting Signature:

A Functional Data Analysis Approach for MQTT 5.0 Protocol

Pavel Koprov, Shyam Gadhwala, Aniket Walimbe, Xiaolei Fang, Binil Starly.

* chapter is based on [1], [2]. The [1] has been published, the [2] is under peer review.

3.1 Introduction

The advent of Industry 4.0 has significantly transformed manufacturing systems through digitalization and the integration of operational technologies (OT) with information technologies (IT) [3]. This evolution towards the Industrial Metaverse and the implementation of DTs emphasizes the critical need for secure data management and the authentication of physical manufacturing assets [4], [5], [6], [7]. The seamless flow of data from physical machines to their digital counterparts, known as the digital thread, underscores the importance of data integrity and security throughout the manufacturing lifecycle. In 2022, the manufacturing sector became a prime target for cyber-attacks, representing nearly a quarter of all such incidents, which highlights the critical need to address these emerging security vulnerabilities [8], [9], [10], [11], [12].

A key challenge in manufacturing cybersecurity is the lack of a reliable method to uniquely identify machines on a network. Traditional identifiers, such as machine serial numbers and MAC addresses, are prone to spoofing and fail to provide a dependable means of machine identification. This gap hampers the traceability of data generated by specific machines. To overcome this issue, our research proposes a novel approach to extract a digital "fingerprint" of manufacturing machines, enabling their unique identification within a network of interconnected machines [1], [2].
Existing authentication methods, such as hardware keys and operator logins, fall short as they authenticate the operator rather than the machine itself. This discrepancy opens avenues for insider attacks and data manipulation, making it difficult to trace data back to specific machine assets. It is critical for machines to establish their identity through unique fingerprints, ensuring that only authorized devices can access sensitive resources and perform designated actions. This measure is vital for mitigating insider threats, which could involve unauthorized access and exploitation of the system by those with legitimate access rights.

The proliferation of DTs within the IIoT introduces additional challenges, particularly in optimizing communication protocols to efficiently bridge the gap between IT and OT. Traditional protocols such as HTTP/HTTPS, while common in manufacturing-specific applications like MTConnect and OPC-UA, exhibit inefficiencies unsuitable for the demands of IIoT. Our focus shifts towards leveraging more effective protocols like MQTT, which relies on a publish/subscribe model to circumvent the drawbacks of continuous polling associated with HTTP/HTTPS, aiming to enhance IIoT system performance and reliability [13].

MQTT's inherent flexibility allows for a diverse range of data transmission possibilities, from minimalistic messages to extensive payloads like video files. This adaptability is further refined by Sparkplug (or Sparkplug B), a specification by the Eclipse Foundation, designed to optimize IoT applications in industrial settings. Despite its advantages, including outperforming traditional protocols like OPC-UA and Modbus in efficiency and enabling encrypted communications, MQTT Sparkplug faces significant security challenges, notably in safeguarding against unauthorized access and insider attacks [14], [15], [16], [17], [18], [19].

Our research underscored the importance of fortifying data security at the onset of data generation in manufacturing assets to enhance the robustness of DTs. By employing machine-
derived physical characteristics for authentication, we aim to bolster the security framework within connected manufacturing systems. Effective data modeling is pivotal in this context, ensuring accurate and unified data formats for cloud-based systems, which in turn supports improved business processes, error reduction, and enhanced collaboration [20].

3.2 Project Goal and Contributions

3.2.1 Overview

This project aims to address the critical challenge of securing machine-floor assets, including CNC machines, robots, and 3D printers, through innovative authentication methods based on the unique physical characteristics of machine assets. By harnessing the inherent physical variations and dynamic operational patterns of these assets, we propose two advanced methods aimed at generating robust digital fingerprints for secure machine identification and authentication.

3.2.2 Project Goals

The primary goal of this research is to investigate and validate the feasibility of using vibration-based signatures as a novel authentication method. We explore two distinct yet complementary approaches:

- **Vibration as Physically Unclonable Functions (PUFs):** Leveraging the unique vibration patterns generated by machinery during operation, which result from natural variations in manufacturing, such as differences in machine parts like motors, frames, and pumps. These vibrations serve as a distinct and unreplicable digital fingerprint, akin to biometrics for humans, enabling precise and secure machine authentication.

- **Unobservable Fingerprinting Signature (UFS) System:** Focusing on the challenge of authenticating machine-generated signatures to ascertain their origin from actual physical assets rather than simulations. Through the innovative use of functional data...
analysis (FDA), this approach develops a sophisticated model tailored for integration with the MQTT Protocol, enhancing machine identity verification in IIoT and Smart Manufacturing contexts.

### 3.2.3 Contributions to Smart Manufacturing

Our contributions to the field of smart manufacturing and cybersecurity are multifaceted, combining theoretical innovation with practical application:

1. **Innovative Authentication Models**: Introduction of vibration PUFs and an FDA-based model for the UFS System, representing a significant advancement over traditional authentication methods. These models are designed to authenticate machine identities based on their inherent physical characteristics and operational dynamics.

   - **Optimization of Machine Learning Models**: Identification of the optimal machine learning model for feature selection and decision-making, supporting the implementation of vibration-based PUFs and enhancing the FDA approach for dynamic and accurate machine authentication.

   - **Comparative and Longitudinal Analysis**: A comprehensive comparison between the proposed models and conventional authentication methods, alongside a longitudinal study assessing the models' sensitivity to equipment wear and operational changes. This analysis underscores the models' robustness and adaptability to the evolving industrial environment.

   - **Integration with MQTT 5.0 Protocol**: Proposal for integrating these advanced authentication methods with the MQTT 5.0 protocol, aiming to secure data transmission within IIoT environments and facilitate the secure exchange of data across IT/OT systems within enterprises.
3.2.4 Implications for Cybersecurity in Industry 4.0

This project not only pioneers in the field of machine identity authentication but also sets a new benchmark for cybersecurity measures in smart manufacturing and IIoT. By providing robust mechanisms for machine identification and authentication, our work contributes significantly to securing the digital thread in manufacturing processes, thereby enhancing the resilience of Industry 4.0 against cyber threats. The integration of our models with industry-standard protocols like MQTT Sparkplug B Protocol further emphasizes the practical applicability and potential of our approaches in transforming cybersecurity practices within the manufacturing sector.

3.3 Literature Review

3.3.1 Advances in Physical Unclonable Functions and Their Application

The concept of PUFs has emerged as a pivotal technology in enhancing cybersecurity through the unique identification of devices. PUFs leverage the inherent physical variabilities in hardware to generate distinctive, irreproducible responses, functioning similarly to biometrics for humans. This section delves into the significant strides made in PUF applications, their challenges, and the broader implications for industrial manufacturing and the Internet of Things (IoT).

Studies by Mehdi and Starly have demonstrated the feasibility of using PUFs for authenticating devices such as 3D printers and CNC machines with high accuracy. However, they also noted environmental sensitivity affecting classification accuracy [21]. The vulnerability of additive manufacturing to impersonation attacks, as shown by Do et al. [22], further underscores the necessity for robust PUF-based authentication mechanisms. In a related vein, Belikovetsky et al. [23] explored the potential of using audio signal analysis to detect deviations in G-Code execution, a common attack vector in manufacturing settings. Their findings indicate that the
inherent physical movement of the machine plays a crucial role in the effectiveness of the PUF, with modifications to the G-Code not impacting the authentication process. This underscores the PUF's resilience to certain types of tampering, making it a promising solution for enhancing cybersecurity in industrial environments.

The exploration of PUFs extends beyond manufacturing equipment. For instance, Ramesh et al.'s application of audio signal analysis for drone authentication achieved a 99.5% accuracy rate, showcasing the versatility of PUFs across different domains [24]. Furthermore, continuous authentication studies by Gascon et al. and Espin Lopez et al. have expanded PUF applications to mobile devices and biometric parameters, demonstrating their potential beyond traditional manufacturing settings [25], [26].

Cheng et al.'s innovative use of electromagnetic interference (EMI) for CPU authentication highlights PUFs' adaptability and precision in device identification [27]. This success in distinguishing devices emphasizes PUFs' applicability in securing IoT devices, increasingly prevalent in industrial settings. Building on this concept, Pham et al. [28] expanded the application of EMI in cybersecurity by utilizing it to identify and classify malware types. Employing Fast Fourier Transform for data preprocessing and Linear Discriminant Analysis as a supervised machine learning model, they achieved an impressive 98% accuracy in malware classification. This exploration into the nuanced capabilities of PUFs demonstrates their extensive utility in cybersecurity, from authenticating legitimate devices to identifying and neutralizing potential threats.

Gul et al. [29] utilized system response times as a fingerprinting mechanism, demonstrating significant operational time differences among devices from different vendors. This approach, supported by machine learning models like Decision Trees and Naive Bayes, achieved high
precision and recall scores, illustrating the granularity with which PUFs can enhance cybersecurity. Further expanding the scope of PUF applications, Ahmed et al. [30], [31] explored the use of sensor noise for generating unique fingerprints. They utilized eight statistical variables derived from sensor signals for model training, employing One-Class Support Vector Machine (OCSVM) for the detection of security attacks—a departure from their earlier use of multi-class classifiers. The model demonstrated variability in sensitivity, ranging from 73% to 93.5%, with an average of 82%, and a specificity between 86.3% and 94.2%, averaging 89.8%. This detailed analysis underlines the precision and adaptability of PUFs in identifying and countering cybersecurity threats, further highlighting their potential in safeguarding digital infrastructure.

As for other popular methods of ML, Ypma et al. [32] showed how Support Vector Data Description could be used for anomaly detection. Still, this study is related to monotonously working assets that do not have varying patterns in their day-to-day activity.

Addressing IoT security, paper [33] introduces a novel ABAC scheme incorporating blockchain technology to tackle vulnerabilities like single-point failures and data tampering. While highlighting the scheme's efficiency and adaptability to IoT devices, the paper acknowledges the challenge of ensuring the authenticity of initial data input into the blockchain system, pointing to the necessity of robust security mechanisms from the point of data generation.

This review underscores the critical role of PUFs in advancing cybersecurity measures across various domains, from traditional manufacturing to the burgeoning field of IoT. Future research should continue to explore these technologies' integration and implementation to safeguard against evolving cyber threats.
3.3.2 Functional Data Analysis

Functional Data Analysis is a branch of statistics that specializes in analyzing data varying across a continuous parameter, encompassing entities like curves, surfaces, and various functional forms. In FDA, data are conceptualized as infinite-dimensional objects, typically manifested through high-dimensional discrete measurements with a strong dependence between adjacent observations. The high dimensionality and interdependency of these observations present unique technical and computational challenges. To address these, FDA utilizes dimensionality reduction techniques, transforming data into a more manageable lower-dimensional space while retaining essential information. This process enhances the efficiency, interpretability, and predictive capability of the analysis. A central technique in FDA is Functional Principal Component Analysis (FPCA), which decomposes functions based on the eigenfunctions of the covariance operator, focusing on those that account for the most variance to achieve efficient dimensionality reduction. In reference [34], the authors illustrate the application of a novel scikit-fda Python package, specifically employed in their work for conducting FPCA on vibration data. This showcases the practical utility of the technique and the software in extracting meaningful insights from complex functional data.

FDA's applications have been extensively documented in biomedicine and agriculture. A systematic review by Ullah et al. [35] highlights its use in time series data analysis, particularly in biomedicine. Similarly, the study on grapevine bunch rot detection using FDA [36] demonstrates its efficacy in agricultural product quality assessment. In biomedical applications, FDA has been instrumental in analyzing complex time-series data. For example, Ramsay and Silverman [37] demonstrated its use in extracting meaningful patterns from medical data, which could be analogous to identifying unique operational patterns in machines for authentication purposes.
These applications underscore FDA's versatility in handling complex data sets, a feature crucial for machine identity authentication in industrial settings.

The concept of using FDA for machine identity authentication, especially in IIoT, is a novel application. The methodology's capability to analyze continuous operational data from machines, as seen in the work by Avohou et al. [38], can be leveraged to create unique machine 'fingerprints'. These fingerprints, derived from patterns in machine-generated data, can serve as a basis for authentication in IIoT environments.

3.3.3 Security of the MQTT Protocol

The MQTT protocol, originally designed for devices with limited resources, prioritizes minimizing the consumption of computing power, energy, and network resources. Its security features, especially in the widely adopted MQTT 3.1.1 version, include basic measures like username and password authentication for client-broker connections. However, MQTT allows for 'anonymous' connections, where clients without usernames can connect if permitted by the broker. Access Control List is a crucial security feature in MQTT, offering different levels of access control: General (for all anonymous clients), User-Specific Topic (for identified users), and Pattern Substitution (for specific users and clients), with configurable permissions for reading, writing, or both. Despite these features, MQTT’s approach to authentication is not scalable and lacks auto-discovery, essential in the Sparkplug B specification. This limitation underscores the challenge of ensuring secure and efficient communication in MQTT-based IoT systems. In addressing machine authentication, insights from fields beyond manufacturing, such as computer identification, system authentication, finance, and mobile telecommunications, are considered to enhance security protocols.
In the study presented in [39], the author critically examines the security limitations associated with data transfer in MQTT protocol version 3.1.1. A particular focus is placed on the protocol's inability to distinctly manage multiple devices controlled by a single user, each with different client IDs. To address this shortcoming, the author proposes an innovative access control model tailored for MQTT. This model empowers users to directly assign access rights to topics via IoT devices, thereby facilitating the establishment of public MQTT gates. A significant feature of this model is that it grants users the capability to claim ownership and set read-write permissions for new topics autonomously, without the intervention of the gate’s administrator. Such a modification in the protocol inherently amplifies its flexibility and substantially enhances user autonomy in the management of topic privileges.

The 2018 release of MQTT 5.0 marked a significant evolution in the protocol's security features, notably through the introduction of the AUTH packet. This enhancement allows for the integration of various third-party plugins to verify client authenticity, illustrating a move towards more robust security measures. However, this increased security comes with added complexity. For example, authentication methods like the Salted Challenge Response Authentication Mechanism (SCRAM) require multiple exchanges of authentication data, rendering the single-exchange framework of the CONNECT and CONNACK packets inadequate for these more sophisticated protocols. To address this limitation, MQTT 5.0 integrates the AUTH packet, facilitating a multi-stage process for exchanging authentication information [40]. Fig. 3.1 in the cited work illustrates this enhanced authentication process in detail, using SCRAM as a representative example.
3.4 Methods

3.4.1 Hardware and Software Setup

In this research phase, we expanded upon our initial experiments to incorporate a diverse array of manufacturing assets, focusing on analyzing their unique vibration patterns for cybersecurity applications. Our selection encompassed three primary types of assets: CNC milling machines (specifically, the Haas VF-2 equipped with a New Generation Control unit), a series of collaborative robots (UR series mounted on the Vention platform), and two models of 3D printers (the Original Prusa MINI+ and the Bambu X1C). These assets were chosen based on their operational characteristics and relevance to the study's objectives.

For data acquisition across all assets, we employed the nine Degrees of Freedom (DoF) Internal Measuring Unit (IMU) MPU-9250, which features a three-axis accelerometer, gyroscope, and magnetometer. This IMU was selected for its comprehensive motion measurement capabilities and compatibility with both I2C and SPI communication protocols. Initially, integration with the Raspberry Pi Pico microcontroller using MicroPython was chosen for its straightforward implementation, despite the lack of existing projects that combined this specific IMU with the Raspberry Pi and Python [1]. Subsequent adjustments in our methodology led to the removal of
the Pico microcontroller from the data transmission process to streamline data capture, achieving a sampling rate of 1 kHz for high-resolution motion data analysis [2].

![Image of hardware setup](https://via.placeholder.com/150)

**Fig. 3.2** Initial (a) and consecutive (b) hardware setup on VF-2 CNC milling machine

To install sensors on the CNC machines, existing threaded holes on the back side of the sheet metal cover were utilized (see Fig. 3.2), selected for their resonant quality during axis movement—a standard feature across all VF-2 machines. We explored two control methods for "password" movements: simultaneous XYZ movement versus individual axis movement, opting for the latter to better isolate vibration patterns for analysis. Two different IMUs were tested on the CNC machines, with no significant differences in measurement signals observed.

For the Original Prusa MINI+ 3D printers, the IMU was strategically mounted atop the Z-axis gantry to capture the maximal vibrations from the servo motors responsible for X, Y, and Z movements. In contrast, the Bambu X1C printers had accelerometers mounted on the back plate, using screw threads intended for spool bracket mounting (Fig. 3.3), a decision made to ensure optimal vibration capture without disrupting printer operations. The "password" movement for
these printers was adjusted to XY plane movements due to the indistinguishable vibration levels of the Z-axis from background noise.

Unlike the CNC machines and 3D printers, the 6DoF UR cobots required a specialized four-waypoint program to facilitate the comprehensive capture of XYZ positional changes while maintaining RPY orientation. The IMU placement and robot interchange were carefully managed to ensure consistent data quality. The Raspberry Pi 4B, used for data processing, was placed adjacent to the testing area.

All hardware setups utilized 3D-printed brackets for mounting the IMU, crafted from carbon-infilled nylon material (Onyx) using a Markforged Mark Two printer. The code for collecting vibrations on the PC is written in Python and exploits libraries pandas, serial, and matplotlib. The user is prompted to input the Machine name and the number of runs in this code. After the number of runs is set, the code calibrates the noise levels. The script contains calibration offset creation for ambient noise/vibration (measured within 1 sec after booting), then triggering the signal that exceeds four standard deviations (SD) above the offset and recording data. If 500 measurements fall below the threshold, then data recording stops. This is made to collect acceleration within 3 SD within the movement cycle and avoid recording some accidental vibrations from the assets. The shift to using the newly released MPU9520 library for Python
significantly enhanced our data processing capabilities, with all code made available in our GitHub repository under the rpi_version branch: https://github.com/pkoprov/CISCO_WBP.

This evolution in our hardware and software setup reflects our ongoing efforts to refine data acquisition techniques for vibration analysis, underscoring the importance of adaptable methodologies in cybersecurity research.

3.4.2 Password Moves

Password moves need to be long enough to catch crucial acceleration patterns that the moving parts of the machinery can produce. If the asset contains several moving axes, it is better to move them all, as it would add more to the total variance of the sample. 3-axis CNC Machines and 3D printers can move one axis at a time to change the tool's location linearly. Such movement involves only one of the servomotors moving at a time. 6DoF robots cannot supply linear movement using only one of the servomotors at a time due to each axis's polar degree of freedom. In this case, the vibration pattern will include the PUF of all the motors at each point of time of the password move.

In the case of material removal by CNC machines, the password move may be implemented at the time of tool changing (but may not be long enough) for the in-process authentication or before the machine starts to run the program.

The G-code program is loaded to the machine before it starts and cannot be modified while running. Hence, this one-time authentication may happen before the program changes. We perform the password move before the program starts for proof of concept. A password move can automatically be added to the G-code in a real-life implementation.

VF-2 milling machines can move up to 30 inches on X-axis, 16 inches on Y-axis, and 20 on Z-axis. To get enough data, the password movement is described as follows:
1. Move 30 inches in X negative direction;
2. Move 15 inches in Y negative direction;
3. Move 30 inches in X positive direction;
4. Move 15 inches in Y positive direction;
5. Move 4 inches in Z negative direction;
6. Turn the spindle 8000 RPM clockwise for 1 second;
7. Move 4 inches in Z positive direction;

The same principle can be applied to 3D printers. For example, some industrial-grade FDM 3D printers, such as the Stratasys F123 series, perform material purging between each layer, which can be used as a verification process and treated as a password move. However, controlling the movement of these printer’s gantries with G-code or other open-source methods is not possible, which poses a challenge for data collection and verification purposes. This issue can be resolved if manufacturers include the option of password movement in their software.

Original Prusa MINI+ printers can be controlled by G-code and easily follow the patterns and feed. The password move uses the max federate of 1 m/s and the max travel in the X and Y axes. Z axis feed rate is much slower and was limited to 20 mm for time purposes. The program starts from the X0 Y0 Z10 position and waits for 2 seconds before each run. The password move is very similar to that of the CNC machine:

1. Move 180 mm in X positive direction;
2. Move 180 mm in Y positive direction;
3. Move 180 mm in X negative direction;
4. Move 180 mm in Y positive direction;
5. Move 20 mm in Z positive direction;
6. Move 20 mm in Z negative direction.
Bambu X1C printers have a larger build plate and thus their program was similar to Prusa printers but with the following endpoint coordinates in XY plane: (0,0), (250,0), (250,250), and (0,250). The feedrate was set at 15 m/s, a decision based on preliminary tests that balanced the need for clear data capture with operational efficiency. The specifics of the “password” moves, including their execution and data capture process, are illustrated in Fig. 3.4.

There are many possible scenarios for robotics password moves. Cobots are mostly used for material handling and perform return movement from one fixed waypoint to another without an active payload. This period can be used as a password move and allows continuous authentication between operations. We chose to perform a simple rectangular path in one plane as a worst-case scenario to study if unique signatures are being created from robot models that look fairly same.

UR robots can perform movements in 3 modes: MoveJ, MoveP, and MoveL [41]. MoveJ mode moves the robot in joint space, creating a smooth path. In this move, we chose to move the Tool Center Point (TCP) in the XY plane, resulting in all joints committing rotations. There were four waypoints created with the following coordinates in mm:

1. 0, -400, 250
2. 300, -400, 250
3. 300, 400, 250
4. 0, 400, 250
All waypoints kept the same RPY 90°, 0°, -90°. Every waypoint has 1 sec to be reached, followed by 5 seconds of dwelling after waypoint 1. The vibration patterns produced by each robot are depicted in Fig. 3.5.

It’s important to emphasize that in practical implementations, each machine should have a unique password move, which ideally represents a specific action performed routinely by the asset. This approach ensures that the security mechanism is closely integrated with the machine’s operational profile, enhancing its effectiveness and relevance. The selection of the password move motion path is randomly identified by the machine itself. It is assumed that this motion path is not previously known by any potential attacker. As in any password move – these moves need to be updated frequently.

Each machine has run this procedure 30 times after warming up the axis motors and the spindle. Every run has been separated by 5 seconds of dwell. This number was determined based on a balance between obtaining sufficient data for robust analysis and the constraints of time and resources. In statistics, a sample size of 30 is often considered the minimum number required to apply the Central Limit Theorem [42]. These measurements were then processed to form upper and lower curves, subsequently represented as FDataGrid objects for analysis. Upon performing FPCA on this data, several outliers were identified. The presence of these outliers necessitated their removal from the dataset, leading to a reduction in the number of samples for some assets. Consequently, the final dataset contained between 28 to 30 samples per asset, slightly less than the initial 30 due to outlier exclusion.
Fig. 3.5 Vibration patterns of UR cobots. Ovals highlight the differences in signals. Black ovals show the difference for UR-10e. Green ovals highlight the difference between 2 similar UR-5e patterns. Purple ovals highlight the difference between the other two similar UR-5e patterns.

Fig. 3.6 Vibration patterns of Prusa 3D printers. Ovals highlight the differences in signals. Each oval circumscribes part of the signal specific to only one printer.

Fig. 3.7 Vibration patterns of VF-2 CNC machines. Ovals highlight the differences in signals.
3.5 Data processing

3.5.1 Using Raw Data

We can see that each asset produces a different vibration pattern performing the same password movement (Fig. 3.5, Fig. 3.6, Fig. 3.7). A computational method of identifying differences is needed.

One of the common ways for signal processing is applying convolutions on time series data. Ing et al. [43] demonstrated simple low-computing touch localization using accelerometers and convolutions. They show that the signal can mathematically be expressed as a convolution product between the emitted signal \(e(t)\) from the touched point \(P\), and the impulse response to the sensor \(S\), \(h_{PS}(t)\):

\[
S(t) = e(t) \otimes h_{PS}(t)
\]

This methodology compares each recorded signal to a benchmark and calculates the normalized score. The signal with the identical score is the convolution of the benchmark signal on itself. If we compare unknown scores – the one with the highest value has a high probability of being received from the same device. In our experiment, this method worked for CNC machines but not for robots. There were cases when the signal was very close in time-acceleration pattern but higher in amplitude, resulting in scores of more than one, which could yield an incorrect prediction.

The SD of the stationary noise for MPU-9250 doesn’t exceed 0.03% (0.0024G) of the range in the mode of ±4G. The program starts registering accelerations only if the reading exceeds 3 SDs in any direction. The recording stops if the signal lasts less than 0.5 seconds after that point. The stationary noise lasts less than the 5\(^{th}\) percentile of the 3D printer, the 8\(^{th}\) percentile of cobots, and the 30\(^{th}\) percentile of CNC machine signals. The main principle for differentiating the signals
between assets is their temporal pattern and not the actual values from the sensor. The relation between values in consecutive is of main importance. Moreover, we collected 30 samples per asset to include most of the variance in our models.

Each password is generated from 4 to 8.5 thousand time steps with acceleration values in the X, Y, and Z axes. This is time series data, and every timestep represents a feature (variable). In our first research all data was fed to the ML models in a pure form with all three axes data. Every run is a row with 12 to 25.5 thousand columns. Non-linear models better fit such data, so we used flexible non-linear tree-type models. In our work, we tested supervised and novelty detection ML methods.

Supervised ML may be applicable when someone wants to identify the asset or authenticate based on binary classification (target and non-target asset) in manufacturing facilities where several identical machine assets are presented. We tested our data on Decision Trees, Random Forests, SVM, and LASSO models. Supervised methods are impossible for cases where the machinery is present only in a single unit, as the non-target class data is not available for training. In the case of anomaly detection or "fingerprinting," one-class classifiers are the better fit. Our work used two novelty detection ML methods: Isolated Forests and One-Class SVM.

We collected 30 samples per machine asset and randomly resampled them with a 3/1 ratio for training and testing purposes. The analysis of data and modeling was performed in RStudio with libraries glmnet (LASSO), rpart (Decision Tree for classification), randomForest, e1071 (SVM), kernlab (OCSVM), and isotree (Isolated Forest).

For supervised methods, data were coded into two classes: the name of the asset and "false." After training, a model made predictions on a testing sample that contained 25% of target class data and all other runs of not included false class assets. The decision for classification in
novelty detection models was made by choosing the threshold of the predicted scores. In the base scenario, a 95% score cutoff was chosen.

3.5.2 Using Functional Data

Instead of synchronizing raw data using both timestamps and cross-correlation, the proposed approach now exclusively relies on timestamps for synchronization. This change is based on the observation that time series data, particularly from the X-axis, distinctively represents the shape of each asset. To standardize the data, each curve was centered at zero by subtracting the mean, ensuring uniformity across different datasets.

Our method was refined to capture the characteristics of the signal more accurately by extracting its upper and lower edges. This is achieved using a 10-millisecond moving window. The process involves creating two separate dataframes: one for values above the zero line (top) and another for values below it (bottom). In these dataframes, values that do not comply with the criteria are replaced with zeros. For each 10-millisecond interval, the upper curve, $U(t)$, is determined by identifying the maximum value in the top dataframe, while the lower curve, $L(t)$, is derived from the minimum values in the bottom dataframe. The process can be mathematically represented as:

$$
U(t) = \max \{X(t') > 0: t - 10ms \leq t' \leq t\} \\
L(t) = \min \{X(t') < 0: t - 10ms \leq t' \leq t\}
$$

This approach effectively reduces the size of the resultant curves to one-tenth of the original dataframe. However, it results in varied time steps. To address this and prepare the data for analysis using scikit-fda, linear interpolation was employed. This step fills in missing points, ensuring a consistent grid in the time domain. The interpolation process is defined as:

$$
U_{\text{interp}}(t) = \text{LinearInterpolate}(X_{t_i}, U_t) \text{ for } X_{t_i} \notin U_t \\
L_{\text{interp}}(t) = \text{LinearInterpolate}(X_{t_i}, L_t) \text{ for } X_{t_i} \notin L_t
$$
Fig. 3.8 illustrates the resulting top and bottom curves post-interpolation. Ensuring consistency in the data grid is a critical aspect of FDA. This uniformity allows for the accurate representation of each data point as part of a continuous curve or surface. It facilitates meaningful comparisons and analyses across different functional objects. A consistent grid is essential for applying statistical methods such as Functional PCA, regression, or classification in FDA. Without this uniformity, these methods might yield skewed or inaccurate results, as they assume that functions are observed or interpolated at common intervals. Therefore, maintaining a consistent data grid is foundational for the integrity and reliability of the analyses in FDA.

Fig. 3.8 Acceleration on X axis time series data plotted for UR robots. Grey lines represent collected data, red and blue curves are the shapes of upper and lower mean bounding shapes.
3.5.3 Training and testing

The functional data (i.e., the top or bottom curves) is denoted as $S_i(t)$, which are independent realizations of a stochastic process $X(t)$ with a mean function $\mu(t)$ and covariance function $C(t,t')$, where $i = 1, \ldots, N$, $N$ is the number of samples in the training dataset, $t, t' \in [0,T]$, $T$ is the length of the curves. Using Mercer’s theorem, the covariance matrix $C(t,t')$ can be expanded as follows:

$$C(t,t') = \sum_{k=1}^{\infty} \lambda_k \phi_k(t) \phi_k(t')$$

(3)

where

$$\xi_{ik} = \langle S_i(t) - \mu(t), \phi_k(t) \rangle = \int_0^T (S_i(t) - \mu(t)) \phi_k(t) dt$$

(4)

for $k = 1, 2, \ldots$ are known as FPC-scores, which are uncorrelated random variables with mean zero and variance $\mathbb{E}(\xi_{ik}^2) = \lambda_k$. In this article, only the first principal component was used to truncate the curves, which yields

$$\tilde{S}_i(t) = \mu(t) + \xi_{i1} \phi_1(t)$$

(5)

In our approach, the FPCA is applied to the training data, which exclusively comprises data from a specific target machine. This process involves extracting the mean function and eigenfunctions (principal components) from the training dataset. The mean function represents the average trend across all samples in the training set, while the eigenfunctions capture the primary modes of variation around this mean. The FPCA on the training data yields a set of eigenfunctions, $\phi_k(t)$, and their corresponding eigenvalues, $\lambda_k$. These eigenfunctions are crucial as they form the basis for expanding both the training and testing data. The training data expansion using these eigenfunctions is straightforward, as it involves the data from the same machine. For the testing phase, the dataset includes both target (data from the same machine as the training set) and non-target data (from different machines). This test data was expanded using the eigenfunctions derived...
from the training set. This expansion is key to transforming the test data into the same functional space as the training data, allowing for direct comparison and analysis.

The critical step in our methodology is determining whether the test data belongs to the machine represented in the training dataset. To achieve this, a metric based on the FPC scores obtained from the test data expansion was computed. Specifically, the test data was projected onto the eigenfunctions from the training set and calculated the FPC scores for these projections. These scores represent how well the test data aligns with the principal modes of variation captured by the training data. The decision metric is computed as follows: first, reconstruct the test data curves using the mean function and the FPC scores (5). Then, calculate the L2 distance between the original test data curves and the reconstructed curves. This distance metric effectively quantifies the deviation of the test data from the expected behavior modeled by the training data.

Fig. 3.9 Original and reconstructed curves. Blue is the original curve and orange is the reconstructed curve from FPCS. The upper plot shows the mean curve for training data (UR5e_N). The middle plot shows the random curve of one of the UR5e_W samples from testing set. The lower plot shows the random curve of one of the UR5e_N samples from testing set.
For intrusion detection or verification purposes, a threshold based on the distribution of L2 distances calculated for the training data was established. Specifically, the 95th percentile of these distances was used as a cutoff. Test data resulting in an L2 distance below this threshold is classified as belonging to the target machine (i.e., the machine in the training dataset), while data exceeding this threshold is flagged as non-target or anomalous (Fig. 3.11, Fig. 3.10, Fig. 3.12). This method ensures that the test data is evaluated based on its conformity to the functional patterns established by the target machine, allowing for accurate and reliable machine verification.

![Performance metrics of initial FPCA and OCSVM models](image)

Fig. 3.10 Performance metrics of initial FPCA (a, b, c) and OCSVM (d, e, f) models of UR robots. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM.
Fig. 3.11 Performance metrics of initial FPCA (a, b) and OCSVM (c, d) models of VF-2 CNC machines. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM.

Fig. 3.12 Performance metric of initial FPCA (a, b, c) and OCSVM (d, e, f) models of Bambu printers. X axis represents sample number, Y axis represents the normalized reconstruction error for FPCA and prediction score for OCSVM.

3.5.4 Evaluation Metrics

This study continues to utilize the key metrics from our previous work to assess the performance of machine learning models, with a particular focus on sensitivity, specificity, and the F1 score. These metrics are critical in cybersecurity applications, where the accurate detection of threats and minimization of false positives are target objectives.
**Sensitivity (True Positive Rate or Recall):**

Sensitivity is paramount in scenarios like cybersecurity where missing a true positive is critical. It measures the model's accuracy in identifying positive instances, calculated as:

\[
Sensitivity = \frac{TP}{TP - FN}
\]  

High sensitivity signifies the model's effectiveness in capturing positive cases, thereby reducing false negatives.

**Specificity (True Negative Rate):**

Specificity assesses the model's ability to correctly identify negative instances. It's essential in reducing false positives, with high specificity indicating effective negative case identification. This metric is especially important in applications where false positives, like in spam filtering, are a major concern. Specificity is calculated as follows:

\[
Specificity = \frac{TN}{TN - FP}
\]

**F1 Score:**

The F1 score balances precision and recall, crucial where both false positives and negatives carry significant weight. It's the harmonic mean of precision and recall, defined as:

\[
F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
\]

where Precision is calculated as: \(\frac{TP}{TP + FP}\).

In the realm of cybersecurity, attaining a high F1 score is indicative of a model's adeptness in accurately identifying true threats (demonstrating high recall) while concurrently keeping false positives (ensuring high precision) to a minimum.

Our study, with a focus on cybersecurity, targets achieving elevated levels of sensitivity and specificity, thereby guaranteeing thorough threat detection alongside a reduction in false alarms. The F1 score plays a pivotal role in gauging the equilibrium between precision and recall,
an aspect that becomes especially critical in datasets with imbalanced classes. Collectively, these metrics furnish a comprehensive evaluation of our model’s effectiveness in real-world cybersecurity scenarios.

3.6 Results

3.6.1 Raw Data and Classic Machine Learning

The performance of ML models is depicted in Table A1 (appendix A1). The Decision Tree model for VF-2 machines always reduced the decision to only one variable, as the difference in this variable was stable and large enough for classification. The Random Forest model primarily uses 4 to 6 variables to decide, and the error reduces to 0 after 50 trees. LASSO reduces the model from 5 to 25 variables depending on the training split (random seed). Unlike other methods, Random Forests take a significantly longer time for training: 34 seconds against 4 seconds for SVM and 0.9 seconds for Isolation Forests. Decision boundaries for novelty detection models IF and OCSVM were chosen in such a way as to reject at max two target class test samples (appendix A2: figures A2.1 and A2.2). As shown in figures A2.1 and A2.2, VF-2_2 has a very tight decision region in the novelty detection models. However, the separation is very distinct, unlike in the case of IF. Supervised ML models for VF-2 CNC machines performed with an outstanding result of 100% accuracy in predicting the classes. This can be explained by the fact that even though they were purchased at the same time and have identical equipment, they were used for different hours and experienced other conditions while cutting. VF-2_1 machine has experienced crashes several times during training sessions with students, and VF-2_2 did not have such events throughout its lifecycle. These conditions predetermined the variety in vibration patterns performing the same password move (Fig. 3.7). Of course, the smaller sample size for only two machines made it easier for supervised ML models to identify the class. On the other hand, novelty detection methods do
not have information on other classes in the training process and showed outstanding results, with the F1 score being more than 95%.

UR robots in the advanced manufacturing lab were used only for research purposes and didn't have many work hours. Neither of them experienced hard crashes. Likewise, in the case of CNC machines, Decision Tree models made decisions by only one variable at the beginning of the signal. Random Forests had a different number of the most important features for the decision process depending on the asset: from 1 to 4. The LASSO model for robots has reduced the model to 1.5 important features. As shown in figure A2.1 (appendix A2), robot R has a tighter decision region in the OCSVM method than other robots. One of the test samples can even be falsely classified as non-target. In the case of IF, the separation is very distinct for every robot (figure A2.2 appendix A2).

Decision Tree models for Prusa 3D printers chose 1 or 2 parameters to make decisions, and their location was all over the signal length. The number of variables important for the decision-making in the RF model was from 2 to 8, with a median of 4.5. LASSO reduced models to have 9 to 29 variables with a median of 18. OCSVM model had shown a wide decision region for all printers except Prusa E. Printer Prusa G also had one test sample that was very close to non-target sample scores (figure A2.1 appendix A2). IF models had a worse performance than OCSVM, where scores for printers E, G, and Q were too close to non-target scores. Some test sample scores for printers E and G intersect with false scores. The decision boundary for the Prusa Q printer had to be manually set because one of the train scores was in the false region.

Overall, SVM and OCSVM performed the best, with the highest sensitivity, specificity, and F1 scores. Additionally, SVM had the lowest training time compared to other supervised models. It was eight times faster on average. OCSVM was slower than IF in training but performed
better and more consistently. A supervised model can be chosen when you have more than four units of identical machinery and they do not differ much. OCSVM is preferred in the case when only one of the asset types is available, or gathering the data from all the assets of the class is not feasible (stopping the conveyor).

3.6.2 Functional Data Analysis

The initial models, derived from outlier-adjusted data, were then utilized for subsequent authentication processes. The performance and results of these initial models are illustrated in Fig. 3.10, Fig. 3.11, Fig. 3.12. A significant separation between L2 errors for all target and non-target samples using FPCA method is observed. All models achieved 100% sensitivity and no lower than 98% F1 score, indicating the proposed method's ability to differentiate intruders every time with a negligibly low rate of rejecting a target machine pattern.

To benchmark our approach, the results were compared with those obtained from the previous best-performing method, the OCSVM. For this comparison, the best models based on a threshold set at the 80th percentile of the testing data were selected. The comparative results are depicted in Fig. 3.10, Fig. 3.11, Fig. 3.12. With this threshold, models achieved 100% sensitivity in almost all cases, except for Bambu_S and UR10e_A. For Bambu_S, a lower threshold is needed to achieve 100% intruders’ rejection, but it will come at the cost of lower specificity. For UR10e_A, the proposed method does not work effectively. The threshold setting in the OCSVM method is crucial but its requirement for manual adjustments is suboptimal, potentially failing to accurately reflect the model's current state.

The performance of both the FPCA and OCSVM methods on the Prusa dataset is included in appendix A2. The FPCA method is shown to have higher performance and reliability compared to OCSVM. In the FPCA method, the threshold is chosen based on training data, which tends to
create a more robust and generalized model. Conversely, the OCSVM method selects its threshold based on testing data. While this may be effective in controlled scenarios, it can be less adaptable and accurate in real-world applications, where data characteristics often vary significantly from the testing set.

Fig. 3.13 and Fig. 3.14 demonstrate the longitudinal performance of the FPCA “old” and updated models over 14 days. For most assets, the “old” model’s error rate increased over time, confirming our hypothesis that models need regular updates due to equipment wear and tear. The only exception was Bambu_S, where the error rate decreased, possibly due to its time series vibration pattern becoming more like the original signature. For the UR robots, data collection was limited to four days due to a malfunction in the UR5e_W cobot. Nonetheless, an increasing error trend was observed.

Fig. 3.13 Longitudinal performance of FPCA “old” models: a) VF-2 machines, b) Bambu printers, c) UR robots. X axis – day, Y axis – the normalized reconstruction error.

In the updated model plots, a notable improvement can be observed in model performance after the threshold is adjusted. Specifically, from day 6 onwards, most assets demonstrate a significant enhancement in model accuracy, with at least one of the attempts being accurately identified. This trend becomes even more pronounced after day 10, by which time all the original
data has been replaced with new samples. At this stage, all models consistently achieve 100% sensitivity and maintain a specificity of at least 90%. This improvement aligns with our hypothesis that updating the training dataset to include at least half of the newly collected data allows FPCA to effectively capture most temporal variances in the data.

Fig. 3.14 Longitudinal performance of FPCA updated models: a) VF-2 machines, b) Bambu printers, c) UR robots. X axis – day, Y axis – the normalized reconstruction error.

However, an interesting observation is made with the Bambu_S asset. Despite the overall trend of improving model performance, the error rate for Bambu_S decreases, leading to a decline in the model's performance. By the end of the observation period, there is a significant drop in the model's sensitivity for this particular asset. This could be indicative of a malfunctioning sensor or a scenario where the features captured by the sensor become increasingly indistinguishable from those of another asset.

Fig. 3.15 demonstrates the models' adaptation to equipment dynamics. For instance, the vibration signature of Bambu_M was recorded while Bambu_S was operating at high speed. Both
printers, located on the same table platform without dampening, exhibit an error in the signal with noise that is above the threshold, yet remain close in the 2nd and 3rd attempts. For the VF-2_1 machine, a 50 kg fixture was installed, and the password move was recorded. The error rate for the model with this added payload is higher than without it but remains below the threshold, indicating the model's ability to adapt to insignificant changes in operational conditions.

For the UR robots, both UR10e_A and UR5e_N performed the designated move with varying payloads. The first three attempts involved the maximum payload for these robots (10 kg for UR10e_A and 5 kg for UR5e_N), followed by three attempts with a 50% reduced payload. The results show that the errors with payload are above the threshold but are still distinct from the errors associated with non-target data, underscoring the models' capability to differentiate between normal and altered operational conditions. Overall, these results underscore the importance of updating models to capture temporal variances and adapt to equipment dynamics, ensuring high sensitivity and specificity in real-world scenarios.

As a result, the integration of MQTT 5.0 with the UFS for machine authentication is can be proposed. During the MQTT 5.0 connection process, the client machine declares its identity and specifies the 'UFS' method in the CONNECT packet [40]. The broker responds with an AUTH packet, prompting the client machine to perform a designated 'password move'. This move...
involves the machine executing a specific operational action, during which it collects vibration data. Important to remember is that in our study, we assumed that machine assets of the same kind were performing the exact same ‘password’ move. This is a highly unlikely scenario, as machine assets even from the same model type will have different motion paths resulting in varying signature patterns. But in the event, they do happen to be exactly the same, our analysis above shows that the signature can be mapped to its originating source. The collected data is sent back to the broker in another AUTH packet. At the broker's end, an application equipped with the FPCA model processes this vibration data, comparing it against known patterns for the declared machine identity. This process facilitates the decision-making on granting access.

3.7 Discussion

The results of our study offer significant insights into the application of FPCA in machine identity authentication, particularly under conditions of equipment wear and tear and operational variance. Our findings highlight the dynamic nature of machine-generated data and the necessity for adaptive models in cybersecurity applications.

A key revelation from our study is the superior performance of FPCA models in terms of sensitivity and specificity compared to the previously best-performing OCSVM models. This superiority is particularly evident in real-world scenarios, where the ability to distinguish between target and non-target data is crucial. The FPCA method, unlike OCSVM, which operates as a 'black box' model, offers a clearer understanding of decision-making processes, primarily due to its reliance on the shape of time-series data for differentiating between assets.

This aspect of explainability is crucial in cybersecurity applications, where understanding the basis of a model's decision-making process is as important as the decision itself. It aids in trust-building among users and allows for more effective troubleshooting and refinement of the model.
The transparency provided by FPCA models, by analyzing the principal components of the data, offers insights into the key features that drive the model's decisions. Furthermore, the use of a training data-based threshold in FPCA models, as opposed to the testing data-based threshold in OCSVM, aligns better with realistic operational settings. It ensures that the model is tuned to the specific equipment it is monitoring, enhancing both the accuracy and relevance of its predictions. The adaptability of FPCA models to changes in data over time is another critical observation. The performance improvement in updated models, particularly after day 10, underscores the importance of regularly refreshing the training dataset with new data. This approach ensures that the models remain sensitive to the latest operational characteristics of the machines, thereby maintaining high accuracy in authentication.

However, our approach of indiscriminately adding three new samples and removing the three oldest ones from the training dataset, regardless of whether they fell within the established threshold, was identified as suboptimal. A more effective strategy for maintaining a sustainable model would be to selectively incorporate new samples into the training dataset based on their adherence to the predefined threshold. This refined approach ensures that only data representative of the current operational state of the machines, and within the expected performance parameters, are used for model updates. Such a method would enhance the model's sensitivity to the latest operational characteristics of the machines, thereby ensuring continued high accuracy in authentication while preventing the model from being skewed by anomalous or unrepresentative data points. Incorporating this selective update policy could significantly improve the robustness and reliability of the FPCA models, making them more adept at handling the dynamic nature of machine-generated data in real-world industrial settings.
The case of Bambu_S, where a decrease in the model's sensitivity over time was observed, serves as a critical example highlighting the complexities involved in machine identity authentication. This decline in performance could be attributed to several factors: a potential malfunction of the sensor, the simplicity of the "password" moves, and the suboptimal placement of the sensor. In the case of Bambu printers, the sensor's location was such that the Z-axis movement of the printer produced vibrations below the noise threshold, leading to its exclusion from the "password" move. This exclusion could have contributed to the oversimplification and reduced effectiveness of the model over time. This situation underscores the importance of continuous monitoring and regular updates to the model. It also highlights the need for a comprehensive approach to sensor placement and movement design in the authentication process. Ensuring that the sensor is strategically positioned to capture a full range of operational vibrations and designing "password" moves that adequately reflect the machine's operational characteristics are crucial for maintaining the accuracy and reliability of the model.

In contrast, our study demonstrated that for the eight Prusa printers, the FPCA model performed exceptionally well. This success can be attributed to the optimal implementation of these key factors – effective sensor placement and well-designed "password" moves. The stark difference in the performance of the FPCA model between the Bambu and the Prusa printers highlights the nuanced challenges in machine identity authentication and the importance of considering all operational variables in model design and implementation.

The study also sheds light on how changes in equipment conditions, such as the addition of payloads or operational speed variations, impact model performance. The ability of the FPCA models to distinguish between normal operations and altered conditions, as demonstrated in the experiments with Bambu printers and UR robots, is critical for effective cybersecurity measures.
It ensures that the authentication system is robust not only against intruders but also against false alarms due to legitimate operational variations. Interestingly, this characteristic of the FPCA models can be viewed as a beneficial "side effect" for monitoring the health and status of equipment, a key aspect of DT’s validation. For instance, if the vibration readings consistently exceed the established threshold, but not by a significant margin, this could serve as an early warning signal. Such occurrences, especially if they happen consecutively, might indicate that there is something abnormal or potentially problematic with the machine asset.

This scenario suggests a dual functionality of the FPCA models: while primarily serving as a tool for cybersecurity and machine identity authentication, they can also function as a diagnostic tool. By flagging subtle yet consistent deviations from the norm, these models can prompt timely inspections and maintenance checks, potentially pre-empting more significant equipment failures or malfunctions. Incorporating this additional utility into the operational framework of DTs could enhance maintenance strategies, aligning with the needs of Industry 4.0, where interconnected systems and smart analytics play a pivotal role in operational efficiency and equipment reliability.

The integration of MQTT 5.0 with UFS in this manner showcases a dynamic and secure authentication process. It aligns with the ABAC approach, diverging from traditional login/password systems. This method provides a robust security layer by utilizing the unique operational characteristics of each machine, making it challenging to replicate or forge. Furthermore, this approach fits seamlessly into the Smart Factory paradigm, leveraging intelligent systems and advanced analytics to bolster both efficiency and security in manufacturing environments. The application of FPCA in this context not only enhances security but also contributes to a more interconnected and intelligent industrial ecosystem.
3.8 Conclusion

This research marks a significant advancement in the field of machine identity authentication, especially within the realms of the IIoT and Smart Manufacturing. Our study's key contributions are rooted in the novel application FDA, a detailed comparative analysis with existing models, a comprehensive longitudinal data analysis adapting to equipment dynamics, and the proposed integration with the MQTT 5.0 protocol.

In this work, we demonstrated that PUFs could be used not only in electronics industries but in large machinery using such attributes as vibration. Supervised machine learning models can be very precise in detecting the classes of the assets but fail when no additional equipment is available for training. Some platforms like CESMII can potentially be used for training purposes if the owners of the machinery are willing to share such data.

On the other hand, novelty detection ML approaches show great performance. They can be easily tuned for the specific asset to allow sensitivity to be 100% allowing specificity to be as low as 93%. These approaches run faster and do not require additional data except their own.

Our approach, leveraging FDA, signifies a paradigm shift in machine identity authentication. By focusing on the intrinsic temporal patterns in machine-generated data, the authors have developed a model that is dynamic, adaptive, and offers greater explainability compared to traditional methods like OCSVM and Isolation Forests. This model's ability to adapt to various operational characteristics of machines and its transparency in decision-making processes position it as a sophisticated alternative in cybersecurity applications. The comparative analysis between our FDA-based model and existing authentication methods, particularly OCSVM, highlights the efficacy of the FDA approach. Our findings demonstrate that the FDA
model excels in sensitivity, specificity, and adaptability to operational challenges in real-world industrial environments.

Our research extends the application of FDA models by conducting a longitudinal study over two weeks. This approach allowed us to assess the sensitivity of the FDA model to wear and tear and operational changes in industrial equipment. The study underscored the importance of regular updates to the training dataset to maintain the model’s accuracy and reliability. The possible limitation of our approach:

1. The effectiveness of our model heavily relies on the quality of data collected from sensors. Malfunctions, misplacements, or degradation of sensors can lead to inaccurate data, potentially compromising the model’s performance. Additionally, the model’s accuracy is contingent on the precision of the “password” moves, which must be consistently executed. In the real-world implementation, this would be similar to a password rejection, and an approved override protocol is initiated.

2. While the model adapts to gradual changes over time, its responsiveness to sudden or rapid changes in machine operations or conditions may lead to authentication rejection, necessitating subsequent retraining. This could be a limitation in highly dynamic industrial environments.

3. Integrating this new authentication method into existing industrial systems and protocols may require significant modifications or upgrades, posing potential barriers in terms of cost and complexity. This is one of the reasons why easily accessible regions of the machine’s asset and independent of the machine controller to ease implementation strategies.

The culmination of our study is the proposed integration of this advanced authentication method with the MQTT 5.0 protocol, aiming to enhance data transmission security in IIoT environments. By embedding the FDA model within the MQTT 5.0 authentication process, one
can ensure a more secure and reliable communication channel for industrial equipment, aligning with the Smart Factory paradigm.

As industries evolve towards more interconnected and intelligent systems, the need for robust and adaptive cybersecurity solutions becomes increasingly critical. Our research contributes to this need by providing a novel, efficient, and transparent method for machine identity authentication. The unique identification of a machine asset is critical to the connected machine scenario, and our methodology highlights a method that is not dependent on a human user manually logging in with his/her information. The machine asset receives its own identity within the system for authentication and authorization protocols. The integration of our model with MQTT 5.0 protocol paves the way for safer and more secure IIoT environments. Future research should focus on further refining this model, exploring its integration with other machine learning techniques, and expanding its application across different types of industrial environments. The potential of this model to serve not only as a tool for cybersecurity but also as a diagnostic tool for equipment health monitoring opens new avenues for research and application in the realm of DTs and predictive maintenance. In conclusion, our study represents a significant step forward in the field of cybersecurity for IIoT. The novel application of FDA in machine identity authentication, combined with its integration into MQTT 5.0 protocol, offers a promising solution to the challenges faced in securing Smart Manufacturing environments.

Acknowledgement

The authors wish to express their sincere gratitude to Cisco for their generous sponsorship, which was instrumental in the initiation and successful completion of this project.
References


CHAPTER 4

Advancing SME Manufacturing Efficiency: Integrating Digital Twins and Computer Vision for Dynamic Production Adaptability

4.1 Introduction

In an era marked by rapid market evolution and a growing demand for customization, the traditional manufacturing paradigms, particularly within small and medium-sized enterprises (SMEs), face significant challenges. These challenges include the inflexibility of robotic systems, costly and time-consuming setup changes, and a scarcity of integration with advanced sensing technologies. Such constraints starkly contrast with the current manufacturing landscape's demands for agility and adaptability. This study introduces an innovative approach to navigate these challenges, focusing on integrating DT and foreseeing Computer Vision (CV) technologies to optimize material handling in CNC machines within the Smart Factory paradigm.

At the core of this research is the development of a flexible robotic/CNC cell as a use case underpinned by DT usage. This system is designed to navigate the complexities of modern manufacturing with unprecedented adaptability, swiftly adjusting to changes in materials, designs, and production demands. This adaptability is vital for SMEs as they navigate the dual pressures of product diversification and shortened product lifecycles, aiming to enhance productivity while redefining the essence of manufacturing efficiency.

This research delves into the synergistic integration of DT and CV technologies within the Smart Factory ecosystem, emphasizing enhancing motion policy planning and visualizing manufacturing processes. By leveraging real-time data analytics, this approach facilitates reactive adaptations and anticipates changes in production requirements, ensuring agility and efficiency in equipment handling. The advanced manufacturing ecosystem envisioned here is built on the
foundation of M2M communication, enabling seamless coordination across various production elements and ensuring optimal operational flow. This framework is designed to significantly reduce setup times and adapt dynamically to new production demands, streamlining the manufacturing process and enhancing overall productivity.

However, the path to a cohesive system integrating DT and CV technologies presents various challenges, notably in achieving precision and adaptability with cost-effective solutions. This study aims to tackle these challenges, offering a blueprint for a manufacturing system that evolves to meet production needs in real-time.

Introducing such technologies into the manufacturing process is not merely an integration of new tools but a reimagining of the manufacturing paradigm itself. This research aims to enhance the operational efficiency and adaptability of CNC machines and contribute to a broader understanding of the implications of DT and CV integration within smart factory operations. Through a detailed literature review that follows, this study will explore the state-of-the-art in DT and CV technologies, highlighting their transformative impact across various sectors, from manufacturing to space exploration, and setting the stage for a future where production systems are as dynamic as the market demands.

In addressing the contemporary manufacturing challenges, particularly for SMEs, the integration of DT technology emerges as a pivotal innovation. NVIDIA's Omniverse platform offers a freely accessible, AI-enhanced DT environment, enabling developers to meticulously design, simulate, and refine products and processes in real time before production. This leap in technology is not just theoretical; major corporations like Siemens, BMW, and Amazon ([1], [2], [3], [4], [5], [6]) have validated its effectiveness through practical application, showcasing significant improvements in manufacturing and industrial operations. For instance, BMW's
utilization of Omniverse in factory planning has streamlined manufacturing layouts and workflows and projected a 30% savings from enhanced facilities planning and process efficiency. Similarly, Amazon Robotics' employment of Omniverse alongside Adobe Substance 3D has revolutionized warehouse operations, elevating efficiency while minimizing the reliance on physical prototypes. These instances underscore the substantial benefits—from predictive maintenance curtailing downtime to efficiency gains and cost reductions across diverse operational domains, including design and supply chain management. Collectively, they attest to the critical role of DT technology in advancing manufacturing safety, efficiency, and planning precision [4], [7].

4.2 Project Goal and Contributions

Flexibility and adaptability have transitioned from luxuries to essential requirements in the rapidly evolving manufacturing landscape. This project primarily focuses on implementing DT technology within the NVIDIA Omniverse, setting a foundation for a new era in process automation. While our main concentration is on harnessing the potential of DT to enhance the efficiency and adaptability of CNC machine operations in the smart factory setting, we also briefly explore the prospects of integrating CV technologies. This approach aims to refine further and extend the capabilities of DTs, providing a comprehensive framework for future innovations in manufacturing automation. Our primary goals include:

1. Identifying and overcoming current limitations in robotic material handling that can be overcome with the help of DTs.

2. Developing a cutting-edge prototype of DT for superior operational efficiency in NVIDIA Omniverse.

3. Providing actionable recommendations for practical implementation in real-world settings.
The contributions of this research are poised to redefine industrial robotics and smart factory operations, marking a significant leap towards more efficient, flexible, and intelligent manufacturing processes. By bridging the gap between advanced technology integration and industrial application, this study aims to catalyze the adoption of DT in manufacturing, heralding a new era of productivity and adaptability in industrial automation.

4.3 Literature Review

Before diving into the comprehensive literature review of various facets of robotics and DT technology, it's crucial to understand the broader context and the transformative impact these technologies have across multiple sectors. Manufacturing equipment, combined with the power of DT technology, is enhancing manufacturing processes and redefining sectors as diverse as space exploration, network architecture, and even agriculture through advanced simulations and real-time collaboration platforms such as NVIDIA Omniverse.

The review is structured into four key sections, each spotlighting major advancement. First, we examine the role of computer vision in robotic manipulation, emphasizing breakthroughs in object tracking and pose estimation. Next, we cover physics simulations' role in DTs, demonstrating their contribution to more precise and efficient operations. The third section focuses on task planning and Sim2Real transfer, showcasing developments to enhance robotic system efficiency. Lastly, we discuss NVIDIA Omniverse's wide-ranging applications, highlighting its influence on process improvement and integrating digital and physical worlds.

4.3.1 Computer vision models for robotic manipulation

The CV domain in robotics has made leaps forward, particularly in object tracking and pose estimation, crucial for enhancing real-time interaction and precision in digital and physical spaces. Redmon and Angelova [8] made strides in bridging the gap between human intuition and
robotic grasp detection using CNNs, simplifying the complexity of 3D grasps by assuming a 2D approach can suffice for robots equipped with RGB-D vision. This presumption allows the adaptation of the AlexNet framework, although it limits the model to scenes with singular, graspable objects and impacts its versatility in more complex environments.

Schmidt et al. [9] introduced DART, which significantly advanced the real-time tracking of articulated objects by extending the signed distance function to such objects and leveraging GPU acceleration. Despite its reliance on predefined models, DART's contributions to DT technologies in manufacturing have been notable, enabling precise real-time tracking essential for operations involving high degrees of freedom, such as robotic manipulators.

The development of PoseCNN by Xiang et al. [10] represents a breakthrough in estimating the 6D pose of objects within cluttered scenes, efficiently handling the variability of object shapes and environmental conditions. Creating the YCB-Video dataset further solidifies this framework's relevance, providing a benchmark for challenging pose estimation scenarios, particularly in automated settings where interaction between physical and digital entities is crucial.

Li et al. [11] advanced pose estimation through DeepIM, an iterative approach to align rendered images with observed ones, demonstrating enhanced accuracy in benchmarks and adaptability to new objects. Similarly, Deng et al. [12] employed a Rao–Blackwellized particle filter in PoseRBPF to separate rotation and translation estimation, achieving precise pose tracking even in objects with complex symmetries, which is vital for delicate robotic tasks.

In addressing the constraints of acquiring labeled training data, Deng et al. [13] demonstrated the potential of self-supervised learning for 6D object pose estimation, utilizing real-world feedback to refine grasp accuracy, a promising direction for enhancing robotic perception and manipulation. Meanwhile, Sudhakar et al. [14] tackled the Sim2Real gap by comparing
synthetic and real-world data, contributing datasets that serve as tools for improving synthetic data generation and ultimately enhancing model performance.

Collectively, these works underscore a pivotal evolution in robotic manipulation technology, emphasizing the practical implications for various industries, notably manufacturing. The transition towards integrating synthetic data with traditional datasets marks significant progress, especially when coupled with self-supervised learning techniques that streamline model optimization. This synergy of approaches, especially with tools like the Nvidia Omniverse Replicator, underscores a future where adaptive, real-time training can meet the dynamic needs of modern manufacturing and beyond.

While the potential of CV in enhancing robotic manipulation is evident, particularly in household settings, its integration with DT for industrial applications presents an untapped opportunity. Current literature focuses largely on CV’s impact on precision and adaptability in non-industrial environments. However, blending CV with DT technologies could significantly transform manufacturing processes, offering advanced, real-time simulation capabilities for DTs and their physical counterparts. This integration promises innovative solutions for manufacturing challenges, highlighting an essential area for future research in industrial contexts.

4.3.2 Physics Simulation for Digital Twins of Robots

Integrating physics in DT technology in manufacturing systems, robotics, and simulations is a burgeoning area ripe for innovation. This review highlights key studies contributing to enhancing digital representations of physical systems, thus improving manufacturing accuracy and robotics advancements.

Qamsane et al. [15] propose a structured DT development methodology for manufacturing based on the System Development Life Cycle (SDLC). Their approach, exemplified through a case
study on vibration data, prioritizes scalability, reusability, and extensibility despite its simplification to a univariate model for broader applicability and future research avenues.

Ratliff et al. [16] introduce the Riemannian Motion Policy (RMP) framework, integrating dynamical systems with Riemannian geometry for a geometrically consistent robot motion generation. This framework significantly benefits DTs in manufacturing by enhancing the simulation of robot movements, which supports improved production planning and efficiency.

Van Wyk et al. [17] discuss Geometric Fabrics, a method that extends classical mechanics using Finsler geometries for more adaptable robotic behavior designs. This approach, enabling robots to adjust movements based on various factors, including velocity, promises to elevate DT simulations with more dynamic robotic behaviors in manufacturing settings.

Lämmle and András Bálint [18] extend MuJoCo's physics simulation to include a model for assembling electrical components, which is crucial for in silico robot training for complex tasks without physical risk. Lämmle et al. [19] also explore simulation-based learning for robotic electrical cabinet assembly, introducing methods for approximating joining forces critical for precise assembly tasks. These innovations enhance the training and transfer of robot controllers between digital and physical environments.

These studies mark significant progress in physics applications within DT technology and robotics. They signal a shift towards smarter, more adaptable manufacturing systems through robust simulation models and DTs, promising more efficient, responsive, and cost-effective manufacturing processes.

Integrating high-fidelity physics simulation into DT technology represents a significant advancement, adding a new dimension to DT modeling beyond traditional data-driven models [19]. This evolution allows for more accurate and dynamic representations of physical systems.
within the DT framework, enhancing the ability to predict and optimize manufacturing processes more precisely. Incorporating these advanced physics-based simulations into DTs could dramatically improve the modeling of real-world industrial scenarios, offering a pathway to addressing complex manufacturing challenges with unprecedented detail and accuracy.

### 4.3.3 Task Planning and Sim2Real Transfer

In robotics and DT, significant strides are being made in task planning and the Sim2Real transfer, focusing on enhancing robotic systems' efficiency and reliability. This research synthesis highlights efforts to refine planning mechanisms and bridge the gap between simulations and physical implementations.

Paxton et al. [20] propose Robust Logical-Dynamical Systems (RLDS), blending behavior trees with theoretical performance guarantees to generate robust, reactive robotic behaviors from sequential task plans. This approach promises to improve DTs by optimizing manufacturing tasks for strategic decision-making and factory efficiency.

Chebotar et al. [21] introduce the SimOpt framework, which iteratively adjusts simulation parameters based on real-world experiences to narrow the Sim2Real gap. Proven in robotic tasks, SimOpt reduces the need for real-world trials, outperforming standard domain randomization techniques and improving the transferability of simulated policies.

Zhao et al. [22] present Sim2Plan, a framework that employs a message-passing pipeline for effective real-world task execution, integrating scene understanding, robot planning, and performance validation. This approach minimizes the need for real-world training, showcasing the feasibility of transferring complex strategies from simulation to reality.

Hofer et al. [23] focus on integrating physical simulation with deep learning to model physical phenomena accurately, emphasizing the importance of Sim2Real transfer. They advocate
for a multidisciplinary approach to overcome the reality gap, highlighting simulation's role as a safe, cost-effective data generation and preliminary exploration method.

These studies underscore the advancements and challenges in robotic task planning and Sim2Real transfer. The research emphasizes simulation's critical role in advancing robotic systems, from robust task planning to refining simulations with real-world insights. Addressing Sim2Real intricacies aims to enable robots to execute complex tasks with greater precision and adaptability, enhancing automation across industries.

While task planning and Sim2Real transfer have advanced, integrating CV to improve these processes in manufacturing settings remains underexplored, suggesting potential for innovations in robot adaptability and task execution precision.

**4.3.4 Applications of NVIDIA Omniverse in Various Sectors**

The NVIDIA Omniverse platform stands out as a revolutionary tool for real-time collaboration and simulation across various sectors, significantly impacting manufacturing and space exploration processes. This comprehensive analysis delves into its diverse applications, underlining its role in streamlining operations, enhancing system visualizations, and bridging the gap between virtual and physical realms.

Hummel and van Kooten [24] illuminate Omniverse's potential for in situ visualization, particularly in manufacturing, where it integrates with tools like ParaView for immediate data manipulation and rendering, optimizing robotic and CNC machine workflows. Li et al. [25] highlight its use in simulating space missions, notably for debris removal, pointing to a sustainable future in space exploration. Lin et al.'s [26] discussion on Digital Twin Networks (DTNs) and 6G showcases Omniverse's contribution to network design and management, enhancing performance and innovation.
Nickpasand and Gaspar [27] recognize its graphical optimization capabilities, noting its emerging status in industries like offshore wind turbine manufacturing. Ullrich et al. [28] advocate for its role in virtual commissioning within industrial metaverses, emphasizing the importance of interconnected manufacturing systems through collaborative DTs. Hölzer et al. [29] benchmark its performance in physics simulations, which is crucial for minimizing the Sim2Real gap in robotics and ensuring the reliability of DTs in industrial applications.

Further research by Inamura on human-robot collaboration [30], Sai et al. on consumer electronics manufacturing [31], and Sterk-Hansen et al. [32] on integrating mechatronics systems with Omniverse underscores its versatility in enhancing interactive experiences and real-time control. Kaarlela et al. [33] and Mirbod and Choi [34] explore its applications in innovative digital workplaces and smart farming, respectively, through Extended Reality (XR) and DTs, showcasing advancements in training environments and CV systems. Lastly, Vescovi et al. [35] propose supporting a modular architecture in self-driving laboratories, highlighting its scalability in scientific research.

NVIDIA Omniverse's widespread applications across different fields underscore its transformative impact. It offers a unified platform that facilitates real-time collaboration and propels the integration of digital and physical worlds toward more interconnected and intelligent systems. While the NVIDIA Omniverse platform has shown its revolutionary capacity for real-time collaboration and simulation across a broad spectrum of sectors, including manufacturing, there remains a significant gap in literature and practice concerning its adoption and utilization by SMEs in manufacturing. The existing studies and applications highlight its potential and implementation in large-scale industries or specialized fields such as space exploration and network management. This leaves a research void on how SMEs in manufacturing can leverage
Omniverse's capabilities to enhance operations, especially considering their distinct operational and resource challenges compared to larger corporations. Exploring Omniverse's applications within SME manufacturing contexts could reveal unique insights into its adaptability, scalability, and impact on smaller-scale operations, pointing towards a vital area for future research and development.

4.4 Methodology

4.4.1 Following ISO 23247 standard: Automation Systems and Integration – Digital Twin Framework for Manufacturing

The ISO 23247 standard provides a structured framework for developing DTs, at the heart of which lie the Observable Manufacturing Elements (OME) [36], [37]. These elements form the crucial link between the physical manufacturing environment and its digital counterpart. This subchapter delves into the application of OMEs in creating a DT for a CNC/Robot cell, particularly using a Haas VF-2 milling machine and a UR10e collaborative robot.

Digital twinning, as per ISO 23247, encapsulates various attributes reflecting the manufacturing assets' physical characteristics, capabilities, and operational statuses. For the Haas VF-2 and UR10e, the DT encompasses:

- **Identifier**: Unique serial numbers or UUIDs distinguish each unit, facilitating precise equipment tracking and management within the DT framework. Both VF-2 and UR10e have serial numbers.

- **Characteristic**: Supports critical planning and simulation tasks with attributes like the UR10e's payload capacity and the Haas VF-2's spindle speed and coordinates, integral for cutting process planning and safe, collaborative operation.
Schedule: Includes detailed operational timelines and job queues for both machines, dynamically updated based on real-time feedback to ensure efficiency and minimal downtime.

Status: Captures real-time operational conditions, including 'idle,' 'running,' and 'error,' alongside sensor data on positions, loads, and speeds.

Location: Defines the spatial positioning within the robot/CNC cell layout, optimizing the material handling process and workflow efficiency.

Report: Logs activities and performance metrics critical for efficiency analysis, preventive maintenance, and operational improvements.

Relationship: Highlights the interaction between the Haas VF-2, UR10e, and other cell elements, including material handling coordination and safety system integration, which feeds into the DT model's continuous updating.

Integrating these attributes into our equipment and processing DTs yields a real-time, comprehensive representation of our manufacturing operations. This aligns with the ISO 23247 standard's OME requirements and empowers stakeholders to navigate and optimize the manufacturing process precisely.

The "Fit for Purpose" concept from ISO 23247 has guided our DT development, ensuring each robot/CNC cell component is detailed enough to meet our manufacturing objectives. This includes real-time monitoring for downtime minimization and leveraging DTs for production planning and scheduling optimization, directly contributing to operational efficiency.

"Synchronization" differentiates DTs from traditional computational models by enhancing equipment and process monitoring through a two-way data flow. The Haas VF-2 and UR10e's DTs are continuously updated in our cell, allowing real-time adjustments that improve productivity. Synchronization methods, whether event-based for the VF-2 machine or time-based for the UR10e
managed by ROS2, are chosen based on manufacturing requirements. MQTT with Sparkplug B specification (MQTT SpB) [38] and ROS2’s use of the Data Distribution Service (DDS) protocol for communication with the UR10e via Real-Time Data Exchange (RTDE) ensure effective bidirectional data exchange.

This level of synchronization aligns with ISO 23247, positioning our robot/CNC cell not just as a digital twinning technology user but as a contributor to its evolution. Our DT framework meets current operational needs and supports future manufacturing technology advancements. Proposed DT is thus both driven and, within NGC limitations, driving, highlighting its active role in operational efficiency and innovation [37].

The ISO 23247 standard establishes a comprehensive framework for manufacturing DTs, organized into four essential layers of domains. These domains are integral to understanding and
implementing DT technology within our robot/CNC cell setup, comprising the Haas VF-2 milling machine and the UR10e collaborative robot (Fig. 4.1):

Observable Manufacturing Domain: This foundational layer encompasses the physical assets of our manufacturing setup, specifically the UR10e robot and the Haas VF-2 CNC machine. These assets are the primary focus of our digital twinning efforts, representing the tangible elements that our DTs aim to replicate and interact with within the virtual space.

Device Communication Domain: The seamless communication between the physical and digital realms is critical to the operation of DTs. This domain is supported by wired and wireless communication technologies, utilizing a variety of protocols to ensure robust and real-time data exchange. Protocols such as Telnet, MQTT SpB, DDS, and RTDE form the backbone of this domain, facilitating the flow of information between our observable manufacturing assets and their digital counterparts.

DT Domain: At the heart of our framework lies the DT Domain, where the virtual representation of our physical assets is created and maintained. This domain is powered by NVIDIA Omniverse, a platform that will be discussed in further detail later. Omniverse provides the tools and infrastructure necessary to develop highly accurate and interactive DTs, enabling simulation, visualization, and analysis in previously unattainable ways.

User Domain: The final layer of our framework is the User Domain, which includes the application developed specifically for our study. This application serves as the primary interface for interaction between the users – whether engineers, operators, or analysts – and the DTs of our manufacturing assets. Through this domain, users can access, manipulate, and gain insights from the DT data, closing the loop between the physical and digital worlds and facilitating informed decision-making based on real-time and predictive analytics.
4.4.2 Building Digital Twin in the NVIDIA Omniverse

Building a DT within NVIDIA Omniverse represents a cutting-edge method to integrate physical and digital manufacturing assets seamlessly. At the heart of this endeavor lies the Universal Scene Description (USD), a versatile framework pioneered by Pixar to exchange 3D graphics data among various digital content creation tools [39]. USD forms Omniverse's cornerstone of object representation, enabling a rich, scalable, and interoperable 3D content ecosystem. In Omniverse, objects are encapsulated as USD assets, which comprehensively cover geometric details, visual appearances, behaviors, relationships, and the organizational structure of the scene. This all-encompassing representation supports complex simulations and interactions, achieving a DT environment of high fidelity and dynamic responsiveness that closely mirrors the actual manufacturing setup.

The journey of constructing a DT in Omniverse typically initiates with importing CAD models – such as STEP, OBJ, or IGES – of physical assets like machinery and robotic arms. Manufacturers often provide 3D models of their products for download. For our DT of the VF-2 milling machine, we commenced by obtaining the model from Haas's official website and making necessary adjustments in Autodesk Fusion 360. The specific VF-2 model at the Advanced Manufacturing Lab at North Carolina State University includes an umbrella tool changer, probing system, coolant system, and chip auger, alongside additional vises mounted on the table and a tool set comprising 20 various tools utilized in the ISE 316 class.

These STEP files, renowned for their detailed 3D modeling data in engineering and manufacturing, are subsequently converted into USD articulations within Omniverse. This transformation process metamorphoses static 3D models into dynamic, articulated DTs capable of simulating real-world physics, operations, and interactions. USD articulations afford meticulous
control over the DT’s components and movements, offering a potent mechanism for analysis, optimization, and predictive modeling in manufacturing.

Fig. 4.2 USD representations of the VF-2 milling machine and UR10e cobot: a) with stage lights and enclosure, b) with VF-2 lights and without enclosure

To convert the Haas VF-2 model into articulations, it is necessary to construct a corresponding structure of USD Xformable primitives (Xform) and joints between them. In Omniverse, every USD object begins as static, devoid of weight and collision properties. Collision objects, defined as impenetrable by other collision objects, and rigid bodies, which are dynamic collision objects subjected to physics calculations, form the basis of physical interactions. Joints, connecting rigid bodies, can only be moved by applied forces, necessitating drive attributes to maintain specified joint positions. Drives – essentially forces – ensure joints remain in designated positions, with stiffness and damping parameters crucial for smooth, oscillation-free movement.

The VF-2's DT, featuring three moving axes (X and Y for the table and Z for the spindle ram), necessitates a tree of Xforms to facilitate prismatic joints for authentic movement in accordance with OME specifications. The incorporation of drive attributes, such as stiffness and damping, into these joints enables precise position control, articulated as follows:

\[ \tau = stiffness \times (q - q_{target}) + damping \times (\dot{q} - \dot{q}_{target}) \]
where $q$ and $\dot{q}$ are the joint position and velocity, respectively. Note that when the system is reduced to a conventional PD controller in the joint position.

All other required elements of the CAD model have been converted to USD Xforms, and joints were added where needed (doors, tool changer, etc.). Beyond the mechanical articulations, the DT’s aesthetic elements – textures and lighting – require attention. Material Description files (MDL) from NVIDIA Omniverse libraries have been applied to achieve a visual fidelity closely matching the real-life VF-2 machine (Fig. 2).

The endeavor to construct a digital representation of the VF-2 machine in Omniverse was time-intensive, necessitating a significant learning curve to master the tools provided by the Omniverse Kit. However, the value of the completed model as a DT becomes evident once the construction phase concludes. These physics-driven models offer versatility, allowing for integration with various applications to accomplish many tasks. This includes training for computer vision, formulating robotic manipulation policies, and conducting reinforcement learning. Moreover, the potential to utilize these models for virtual reality-based personnel training opens up new avenues for immersive and interactive learning experiences.

The integration of Isaac Sim version 2023.1.1 has significantly facilitated the development of DTs for UR robots, including the UR10e and the Robotiq Gripper 2F-140, which are integral OMEs in our setup. This version of Isaac Sim comes equipped with USD articulation for these components, thereby streamlining the initial model-building process. Additional adjustments were necessary to adapt the DT for use with a Vention platform and ensure all necessary joints were accurately represented.
Distinct from the process used for the VF-2 machine, the UR10e robot leverages ROS2 for control. This transformation into a fully interactive DT – capable of both driving and being driven by external inputs—necessitates compiling several critical files:

1. Universal Robot Description File (URDF): The URDF is an XML format file that details the robot's physical configuration, including its joints, links, and physical properties. It acts as a foundational element in ROS2 for depicting the robot's structure and kinematics, facilitating the simulation of its motion and interaction within a physics-based environment. For our DT, the UR10e URDF provided by Isaac Sim was enhanced by adding the Vention platform and Robotiq gripper, complete with the required transformations. This adaptation ensures that our DT accurately reflects the robot's setup and capabilities, allowing for a more realistic and comprehensive simulation within the Omniverse environment.

2. Lula Robot Description File: Integral for utilizing Lula algorithms with the URDF for our UR10e DT, the robot_description.YAML file delineates the robot's configuration space. It differentiates between "Active" joints, which are subject to direct control by algorithms such as RMPflow, and "Fixed" joints, which are considered immovable. This file is pivotal for establishing the DT's operational parameters, setting default positions for active joints, and detailing collision spheres to facilitate safe navigation and obstacle avoidance within the Omniverse environment. Proper configuration of this file is vital for enabling the DT's interactive capabilities and ensuring simulations accurately reflect the robot's physical operations. The file provided by Isaac Sim includes only the UR10e configuration and requires modifications to integrate the Robotiq gripper. Fortunately, Isaac Sim's Robot Description Editor app simplifies this process, allowing for straightforward edits.
3. RMPflow Config File: RMPflow is an advanced framework designed to create motion policies tailored to robotic systems. The RMPflow configuration file outlines these policy parameters, guiding the robot's movements and reactions to stimuli. Such detailed configuration is pivotal in formulating complex control algorithms, which are fundamental in dictating the robot's behavior. As a result, it enables the DT to emulate real-world physics and the nuanced dynamics of robotic movement accurately. Beyond defining RMP parameters, this file also sets restrictions on potential collisions between the robot and its base. To fully accommodate the UR10e's integration with the Vention platform and address collision scenarios involving the robot's links and the Robotiq gripper, modifications were necessary for the initial file provided by Isaac Sim. These additions ensure a comprehensive representation of the robot's operational envelope and enhance the DT's interaction fidelity within the Omniverse.

The compilation and integration of these files are paramount for several reasons. Firstly, they enable the DT to accurately replicate the UR10e's physical and operational characteristics, ensuring that simulations reflect real-world conditions. Secondly, they allow for advanced simulations involving CV, robotic manipulation, and reinforcement learning by providing a detailed and manipulable model of the robot.

Expanding upon the synchronization aspect of integrating the VF-2 milling machine with its DT in the Omniverse environment, our approach builds on the foundational methodologies established in our prior work [38]. The crux of this integration involves the real-time translation of operational data from the VF-2 milling machine – specifically, the XYZ coordinates, spindle speed, and the identifier of the tool currently in use – into actionable inputs for the DT within the Omniverse USD model.
We utilize an MQTT client that adheres to the Sparkplug B specification to facilitate this real-time data synchronization. It is renowned for its robustness in industrial applications for its structured data and namespace organization. This client subscribes to predefined topics that represent the various operational parameters of the VF-2 machine. Upon receiving updates on these topics, the client forwards the pertinent information to a dedicated control script. This script adjusts the drives of the VF-2’s USD articulation in Omniverse, mirroring the physical machine's real-time operations in its digital counterpart.

This synchronization mechanism indicates the pivotal role that the unified namespace concept, as supported by MQTT Sparkplug B, plays in the realm of DTs. It underscores the potential for replicating the operational state of a single VF-2 milling machine and extending this capability to multiple machines. By subscribing to MQTT topics corresponding to different VF-2 machines, one can achieve a scalable model that allows for the seamless generation of high-fidelity DTs for each machine. Such a model offers significant versatility, enabling users to monitor and interact with any specific VF-2 machine's DT by simply adjusting the MQTT subscriptions to reflect the unique operational data streams of the machine in question.

The data synchronization between the UR10e OME and its DT is facilitated by the ROS bridge application provided by NVIDIA Omniverse. This integration ensures that the DT of the robot accurately reflects the state of the physical OME, leveraging the RTDE-DDS flow within ROS2. As a result, every change in the physical robot's state is immediately communicated to Omniverse through the bridge app, ensuring real-time synchronicity between the physical and virtual environments.

Vice versa, any actions performed with the robot in Omniverse can be mapped to the real robot, allowing for an interactive and bidirectional flow of information. This capability is crucial
for implementing simulated controls and testing scenarios within Omniverse that can be directly applied to the physical robot. It opens up possibilities for remote operation, automated control testing, and fine-tuning robot behaviors in a safe and controlled virtual environment before execution in the real world.

### 4.4.3 Enhancing Event-Driven Behavior with MQTT SpB Protocol and Isaac Cortex

Isaac Cortex, developed as part of NVIDIA's Omniverse platform, serves as a sophisticated decision framework to enhance the programming and operation of collaborative robots, or "cobots." This technology is pivotal in bridging the gap between virtual simulations and physical robotics, providing a comprehensive system that ties together various robotic tooling within Isaac Sim to create cohesive, collaborative robotic systems. Its innovative approach enables easier programming of cobot tasks, akin to programming game AI, by leveraging a belief representation of the world. This representation acts similarly to a robot's brain, where both real and simulated data can be inputs for generating appropriate actions. As such, Isaac Cortex represents a significant step forward in developing, testing, and training AI-powered robots, promoting task-aware and adaptive skills that are crucial for the next generation of robotic automation [41].

Incorporating Isaac Cortex into the operational framework of our system significantly enhances the capability for event-driven behavior, which is enabled through the MQTT SpB protocol (Fig. 4.3). Additionally, the control and operational efficiency of the system can further be elevated by utilizing Large Language Models (LLMs). By generating CMD messages, LLMs facilitate direct communication and command relays to the DTs of assets within the framework. This innovative approach allows for more dynamic and intelligent decision-making processes, where the LLMs can analyze complex scenarios and issue precise operational commands, ensuring that the system's responses are contextually relevant and optimally timed. For instance, initiating
the machine tending process, where the robot performs a pick-and-place task to load stock into the CNC vise, is not only informed by the precise location data provided by the VF-2’s DT within Omniverse but also by the strategic analysis and commands generated by LLMs. This sequence of operations leverages the Cortex framework, employing its sophisticated 6-stage processing pipeline to inform each action, effectively making Omniverse the System's central intelligence, or "mind." Through this integration, our proposed system can harness the advanced capabilities of LLMs to complement the MQTT SpB protocol, thereby enhancing the robot's ability to execute tasks based on a deeper understanding of the operational context and achieving unprecedented levels of automation intelligence.

![Diagram of Cortex Architecture]

1. Perception: camera feed and sensor data
2. World Model: Omniverse DTs
3. Logical State: VF-2 table, stock and robot end effector locations; process state;
4. Decisions: robot motion policy and VF-2 program selection
5. Command API (policies): waypoints generation for UR10e movement
6. Control: ROS2 communication with robot to render the machine and set macros to tune respective G-code

Fig. 4.3 Incorporating Isaac Cortex architecture into our robot/CNC cell DT

Perception and World Modeling stages are crucial as they process sensory streams and populate our USD database with a comprehensive model of the world. This world belief,
visualizable within Omniverse, informs the system about the environment's current state and provides a dynamic window into the robot's "mind."

The Logical State Monitoring phase records the environment's logical state, such as the open or closed status of doors or the presence of an object in the gripper, directly impacting subsequent actions.

In Decision Making, the system leverages the detailed world model and logical state to decide on the next steps. This is where commands to initiate tasks like the machine tending process are formulated, driven by a hierarchical Decider Network that prioritizes actions based on the system's current state and objectives.

The Command API and Control layers then translate these decisions into actionable policies, governing behavior with parameters like target positions and motion commands, ensuring synchronized execution with the physical robot.

Layers 2 through 5 (world, logical, decisions, commands) operate based on the belief model – the simulation running within the robot's "mind" – allowing the design of complex systems entirely in simulation first. This approach focuses on shaping system behavior before integrating with the physical or simulated world, with perception and control aspects being rigorously tested in simulation via synthetic sensor data to emulate real-world conditions accurately.

Cortex's distinction between belief and sim (or real) worlds is instrumental, operating on a belief simulation while potentially paralleling an external simulation or the actual physical environment. This dual-world concept allows for a seamless transition from virtual to real, ensuring that the physical robot can accurately map and execute every action performed in Omniverse, bridging the gap between simulation and tangible execution with unprecedented fidelity and intelligence.
4.5 Discussion and Conclusion

This study set out to address pressing challenges within the manufacturing sector, particularly focusing on the operational efficiency and adaptability of CNC machines in the context of SMEs. By integrating DT technologies within a flexible robot/CNC cell, we embarked on a pioneering exploration to enhance the Smart Factory paradigm. This journey was grounded in developing and operationalizing a system designed to swiftly adapt to the changing demands of production, highlighting the potential for significant advancements in manufacturing agility and responsiveness.

4.5.1 Reflecting on Project Goals and Contributions

Overcoming Limitations with DT Technology: Our project has identified key areas where robotic material handling can be significantly improved beyond the constraints of conventional methods. Traditionally, operators manually configure waypoints for industrial applications, which is time-consuming and prone to inaccuracies. Our innovative approach showcases how these critical tasks can be efficiently delegated to AI-based systems, harnessing the capabilities of DTs. By integrating AI with DT technology, we have outlined a method where the planning and execution of robotic handling are dynamically optimized in real-time, demonstrating a transformative leap towards smarter, more adaptive manufacturing processes.

Development of a Cutting-edge Prototype: The construction of a prototype that seamlessly integrates DT technologies marks a pivotal accomplishment within our project. As a proof of concept and a beacon illuminating the path forward, this prototype demonstrates the practicality and advantages of DT integrations within real-world manufacturing. Our efforts lay the groundwork for subsequent explorations into DT applications in conventional manufacturing environments to achieve smart factory standards. The utilization of specific tools in our project
underscores the potential for SMEs to embrace and benefit from cutting-edge Smart manufacturing technologies, positioning them to compete on equal footing with industry giants.

Actionable Insights and Framework for Implementation: Our research has meticulously crafted a comprehensive blueprint for embedding DT technologies within manufacturing processes, employing advanced tools like NVIDIA Omniverse and Isaac Sim. The strategies and insights derived from our study equip SMEs with actionable methodologies to uplift their production capabilities, heralding a new era in the practical deployment of these innovations in the manufacturing sector. We advocate for equipment manufacturers to adopt the Universal Scene Description (USD) format for sharing CAD models and USD assets. This transition will expedite the adoption of DT technologies, enabling customers to more swiftly design future-ready production systems and aiding manufacturers in enhancing their R&D through direct access to DTs of their equipment on the shop floor.

While our work did not implement CV solutions directly, the potential for CV to amplify the efficacy of DTs is clear. Utilizing the Isaac Cortex workflow, CV can enrich the DT cell by accurately identifying and positioning objects within Omniverse, thus enhancing AI-driven decision-making processes. The ability to detect and localize personnel paves the way for more integrated human-machine collaboration, optimizing the workspace for both entities. Given the less stochastic nature of manufacturing environments, CV systems can deliver more reliable classifications and predictions, accelerating their adoption for material handling and M2M communication.

Envisioning a practical application, machines might communicate through MQTT SpB and LLMs. For instance, upon receiving an order, LLMs could direct robots to select the optimal stock sizes within reach. Decisions informed by CV data would guide the selection and placement of
materials in CNC machines, integrating all necessary assets as USD Xformables and articulations for online planning. Successful DT processes would culminate in physical actions via the Cortex API, setting the stage for seamless operational flows from material handling to CNC tending, including automatic tool changes and precise offset settings for subsequent operations.

4.5.2 Future Directions

Building upon the foundations laid by this study, future research can explore several promising avenues:

Advanced AI and Machine Learning: Investigating the incorporation of AI and machine learning algorithms could further enhance DT's decision-making capabilities and adaptability, offering new ways to optimize manufacturing processes.

Scalability and Industry-Wide Application: Expanding the scope of this research to explore the framework's applicability across various manufacturing settings and industries could uncover the broader implications of DT and CV technologies, driving widespread adoption and innovation.

4.5.3 Conclusions

This research marks a pivotal stride in harnessing the full spectrum of DT (DT) technology within the manufacturing sector. By deploying a flexible manufacturing cell empowered by DT, we have charted a course toward a new standard in manufacturing - one that is more adaptable, efficient, and smarter in its operations. Our exploration into the integration of DT, specifically focusing on AI's role in refining robotic material handling, demonstrates a significant shift toward manufacturing processes that are dynamically responsive to production demands.

By developing a cutting-edge DT prototype within the NVIDIA Omniverse and illuminating potential integrations with CV, our work is a cornerstone for future advancements in smart manufacturing. The construction of a comprehensive blueprint for DT integration offers
SMEs a tangible pathway to elevate their production systems, bridging the technological divide between small enterprises and industry leaders. Moreover, our advocacy for equipment manufacturers adopting the USD format underscores a critical step toward the widespread application of DT technologies, promising to accelerate the design of future-ready production systems.

While direct implementations of CV solutions were beyond our project's scope, the outlined potential for their synergy with DT highlights an exciting frontier for smart factory operations. Envisioning a manufacturing ecosystem where machines communicate through advanced protocols and AI-driven decision-making informs operational strategies, we foresee a transformation in how manufacturing entities interact, collaborate, and evolve.

As we stand on the brink of a new era in manufacturing innovation powered by the capabilities of DT and the untapped potential of CV, the path forward is both exhilarating and daunting. Our advancements beckon further exploration and development, aiming to unlock fully autonomous smart factories. This endeavor, rich with challenges and opportunities, invites the collective effort of researchers, practitioners, and industry stakeholders to continue the journey toward realizing the expansive benefits of DT and CV technologies in manufacturing.
References


CHAPTER 5

Conclusions & Future Work

5.1 Overall Summary & Research Contributions

The evolution towards Industry 4.0 has catalyzed the integration of cutting-edge technologies such as DTs, advanced communication protocols, and cybersecurity measures to create a resilient and efficient manufacturing landscape. This dissertation has explored the synergies between these elements, focusing on enhancing the efficacy of smart factory operations through the innovative application of MQTT Sparkplug B protocol, Unobservable Fingerprinting Signature for machine identity authentication, and the practical deployment of DT in conjunction with computer vision systems within NVIDIA Omniverse for CNC machine optimization.

The significance of this study lies in its holistic approach to addressing the technological and security challenges within Industry 4.0 frameworks. By leveraging MQTT Sparkplug B for seamless data streaming and fostering a unified namespace, this research underscores the protocol's lightweight architecture and flexibility, essential for the rapid configuration of smart factory operations. Furthermore, the novel method of Unobservable Fingerprinting Signature emerges as a pivotal advancement in cybersecurity, offering a robust mechanism for authenticating manufacturing machines beyond conventional identifiers, thereby enhancing data integrity and mitigating insider threats effectively.

The integration of DT and computer vision systems, exemplified through NVIDIA Omniverse, highlights the potential of these technologies in revolutionizing material handling processes for CNC machines. This application not only demonstrates a significant leap towards adaptive and efficient manufacturing processes but also illustrates the practical benefits of DTs in facilitating real-time decision-making and operational optimization.
Overall, the contributions of this study include:

- **In-depth Exploration of MQTT Sparkplug B Protocol**: The study provides a detailed examination of the MQTT Sparkplug B protocol, highlighting its flexibility, lightweight architecture, and suitability for smart factory operations. This work contributes to the field by showcasing the protocol’s potential in creating a unified namespace for seamless data streaming, which is crucial for the rapid configuration and efficient operation of smart factories.

- **Development of Unobservable Fingerprinting Signature for Machine Identity Authentication**: This research introduces a novel cybersecurity mechanism that significantly enhances the authentication of manufacturing machines. The Unobservable Fingerprinting Signature method addresses a critical gap in the current understanding and implementation of machine identity verification, offering a robust solution to enhance data integrity and mitigate insider threats effectively.

- **Practical Implementation of DT Technology**: The dissertation presents a real-life case study demonstrating the practical application and benefits of DT technology, particularly when integrated in the NVIDIA Omniverse platform. This case study provides actionable insights and guidelines for industries, illustrating the technology's potential in optimizing material handling processes and operational decision-making for CNC machines.

In essence, this research bridges the gap between theoretical advancements and practical applications within the sphere of Industry 4.0, laying the groundwork for future explorations that will further intertwine the digital and physical realms of manufacturing. It marks a significant step towards realizing the full potential of smart factories, where technology not only optimizes production but also secures and empowers the manufacturing ecosystem in unprecedented ways.
5.2 Future Work

In light of the research findings and the emerging trends in smart manufacturing, several avenues for future work have been identified. These directions not only aim to build upon the current research but also to explore innovative applications of technology to enhance the capabilities and efficiency of smart factories.

5.2.1 Implementation of Computer Vision Systems

Future research should explore the implementation of advanced computer vision systems to augment material handling processes and facilitate seamless human-machine collaboration. This includes developing algorithms for real-time object recognition, spatial navigation, and safety protocols to ensure a harmonious working environment where humans and machines augment each other's capabilities. Such systems would significantly improve the efficiency and adaptability of manufacturing operations, enabling more flexible and responsive production lines.

5.2.2 Exploiting High-Fidelity Simulation Environments for Training RL Models

The exploration of high-fidelity simulation environments, such as the Omniverse platform, for training RL and CV models presents a promising avenue for future research in smart manufacturing. By leveraging these sophisticated simulations, which offer realistic physics and graphics, models can be trained on synthetic data that closely mirrors real-world scenarios. This approach has demonstrated potential in significantly improving the models' abilities for smarter decision-making and developing agile CV solutions. The advantage of using synthetic data lies in its capacity to enhance model training efficiency, allowing for the rapid deployment of solutions at a scale and speed previously unattainable. Future investigations into optimizing these models for manufacturing contexts could revolutionize how smart factories operate, making them more efficient, adaptable, and capable of addressing complex operational challenges.
5.2.3 Integration with ERP and MES for AI-Driven Decisions

The deeper integration of M2M communication into higher-order systems such as Enterprise Resource Planning (ERP) and Manufacturing Execution Systems (MES) represents a critical area for future exploration. By leveraging AI, these systems can process real-time data from the manufacturing floor to make intelligent, actionable decisions, thereby optimizing production schedules, reducing downtime, and enhancing overall operational efficiency. Future work should focus on the development of interoperable standards and protocols to facilitate this integration, alongside the creation of AI models capable of interpreting complex datasets to drive decision-making processes.

5.2.4 Leveraging LLMs in Manufacturing

The application of LLMs in manufacturing settings to drive higher-level autonomies offers a promising research direction. LLMs can be utilized to analyze vast amounts of textual data within the manufacturing domain, including maintenance logs, operation manuals, and production reports, to generate insights, predict outcomes, and even automate decision-making processes. Investigating use cases where LLMs contribute to areas such as predictive maintenance, quality control, and operational planning could significantly advance the autonomy and intelligence of smart manufacturing systems.

5.2.5 AI-Driven Applications Leveraging Transformer Models

The utilization of transformer models to train AI on videos and extensive datasets accumulated from manufacturing operations presents an opportunity to democratize operations in SMEs. By leveraging these models, AI can learn from complex, multimodal datasets to understand and optimize manufacturing processes, assist in design and innovation, and even conduct quality assurance through visual inspection. Future research should aim to develop frameworks and
platforms that enable SMEs to easily adopt and benefit from these AI-driven applications, reducing the barrier to entry and fostering innovation across the manufacturing industry.

5.3 Conclusion

This dissertation contributes to the advancement of Industry 4.0 by providing a comprehensive analysis and practical applications of DTs, MQTT Sparkplug B protocol, and Unobservable Fingerprinting Signature for machine identity authentication. These contributions not only pave the way for more resilient and efficient smart manufacturing operations but also offer a blueprint for future innovations in this rapidly evolving field. As we look towards the horizon of Industry 4.0, it is evident that the integration of these technologies will play a crucial role in shaping the future of manufacturing, heralding an era of unprecedented operational excellence and cybersecurity assurance.
APPENDICES
Appendix A1

Table A1. Sensitivity and specificity of tested ML models for every asset.

<table>
<thead>
<tr>
<th>Sensitivity/Specificity/F1 score</th>
<th>UR-10e_A</th>
<th>UR-5e_C</th>
<th>UR-5e_N</th>
<th>UR-5e_R</th>
<th>UR-5e_W</th>
<th>VF-2_1</th>
<th>VF-2_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision tree</td>
<td>0.96/1/0.98</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>0.99/1/0.99</td>
<td>1/0.83/0.97</td>
<td>1/1/1</td>
<td>1/1/1</td>
</tr>
<tr>
<td>Random Forest</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
</tr>
<tr>
<td>LASSO</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
</tr>
<tr>
<td>SVM</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>0.99/1/0.99</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
</tr>
<tr>
<td>OCSVM (95% threshold)</td>
<td>1/0.93/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.93/0.97</td>
<td>1/0.93/0.97</td>
<td>1/0.93/0.97</td>
</tr>
<tr>
<td>Isolated Forest (95% threshold)</td>
<td>1/0.93/0.99</td>
<td>1/0.9/0.99</td>
<td>1/0.9/0.99</td>
<td>1/0.89/0.98</td>
<td>1/0.9/0.95</td>
<td>1/0.93/0.97</td>
<td>1/0.93/0.97</td>
</tr>
</tbody>
</table>

continued

<table>
<thead>
<tr>
<th>Sensitivity/Specificity/F1 score</th>
<th>Prusa_B</th>
<th>Prusa_E</th>
<th>Prusa_F</th>
<th>Prusa_G</th>
<th>Prusa_H</th>
<th>Prusa_J</th>
<th>Prusa_P</th>
<th>Prusa_Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision tree</td>
<td>0.85/0.78/0.92</td>
<td>0.83/0.88/0.94</td>
<td>0.89/1/0.94</td>
<td>0.99/0.75/0.99</td>
<td>0.91/1/0.95</td>
<td>0.99/0.83/0.99</td>
<td>0.92/1/0.96</td>
<td>0.94/0.89/0.96</td>
</tr>
<tr>
<td>Random Forest</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/0.88/0.99</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/0.89/0.99</td>
</tr>
<tr>
<td>LASSO</td>
<td>0.97/1/0.99</td>
<td>0.94/1/0.97</td>
<td>1/1/1</td>
<td>1/0.88/0.99</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>0.99/0.89/0.99</td>
</tr>
<tr>
<td>SVM</td>
<td>1/1/1</td>
<td>0.97/1/0.99</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
<td>1/1/1</td>
</tr>
<tr>
<td>OCSVM (95% threshold)</td>
<td>1/0.94/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.94/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.94/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.94/0.99</td>
<td>1/0.94/0.99</td>
</tr>
<tr>
<td>Isolated Forest (95% threshold)</td>
<td>1/0.9/0.99</td>
<td>0.52/0.93/0.67</td>
<td>1/0.93/0.99</td>
<td>1/0.93/0.99</td>
<td>1/0.94/0.99</td>
<td>1/0.89/0.99</td>
<td>1/0.94/0.99</td>
<td>1/0.9/0.99</td>
</tr>
</tbody>
</table>
Appendix A2

Fig. A2.1 Decision boundaries for OCSVM. Blue circles represent training scores. Red circles represent test scores for target data, and empty circles represent non-target data. The red line is the decision boundary. The test score is a raw scoring function of the samples returned by the OCSVM model.
Appendix A2

Fig. A2.2 Decision boundaries for IF. Blue circles represent training scores. Red circles represent test scores for target data, and empty circles represent non-target data. The red line is the decision boundary. The red dashed line is the boundary chosen manually. The test score is a raw scoring function of the samples returned by the IF model.
Fig. A3.1 Performance metric of initial FPCA and OCSVM models of Prusa printers
Appendix A3

Fig. A3.2 Performance metric of initial FPCA and OCSVM models of Prusa printers - continued