Ubiquitous Control of a CNC Machine: Proof of Concept for Industrial IoT Applications

Aebersold, S. A., Akinsolu, M. O., Monir, S., and Jones, M. L.

information

MDPI

Article

Ubiquitous Control of a CNC Machine: Proof of Concept for Industrial IoT Applications

Stefan A. Aebersold, Mobayode O. Akinsolu *, Shafiul Monir and Martyn L. Jones

Faculty of Arts, Science and Technology, Wrexham Glyndŵr University, Wrexham LL11 2AW, UK;
s.aebersold@outlook.com (S.A.A.); s.monir@glyndwr.ac.uk (S.M.); martyn.jones@glyndwr.ac.uk (M.L.J.)
* Correspondence: mobayode.akinsolu@glyndwr.ac.uk or m.o.akinsolu@ieee.org

Abstract: In this paper, an integrated system to control and manage a state-of-the-art industrial computer numerical control (CNC) machine (Studer S33) using a commercially available tablet (Samsung Galaxy Tablet S2) is presented as a proof of concept (PoC) for the ubiquitous control of industrial machines. As a PoC, the proposed system provides useful insights to support the further development of full-fledged systems for Industrial Internet of Things (IIoT) applications. The proposed system allows for the quasi-decentralisation of the control architecture of conventional programmable logic controller (PLC)-based industrial control systems (ICSs) through data and information exchange over the transmission control protocol and the internet protocol (TCP/IP) suite using multiple agents. Based on the TCP/IP suite, a network device (Samsung Galaxy Tablet S2) and a process field net (PROFINET) device (Siemens Simatic S7-1200) are interfaced using a single-board computer (Raspberry Pi 4). An override system mainly comprising emergency stop and acknowledge buttons is also configured using the single-board computer. The input signals from the override system are transmitted to the PROFINET device (i.e., the industrial control unit (ICU)) over TCP/IP. A fully functional working prototype is realised as a PoC for an integrated system designated for the wireless and ubiquitous control of the CNC machine. The working prototype as an entity mainly comprises a mobile (handheld) touch-sensitive human-machine interface (HMI), a shielded single-board computer, and an override system, all fitted into a compact case with physical dimensions of 300 mm by 180 mm by 175 mm. To avert potential cyber attacks or threats to a reasonable extent and to guarantee the security of the PoC, a multi-factor authentication (MFA) including an administrative password and an IP address is implemented to control the access to the web-based ubiquitous HMI proffered by the PoC.

Keywords: industrial IoT; industrial machines; internet; PROFINET; programmable logic controller

Citation: Aebersold, S.A.; Akinsolu, M.O.; Monir, S.; Jones, M.L. Ubiquitous Control of a CNC Machine: Proof of Concept for Industrial IoT Applications. *Information* **2021**, *12*, 529. https://doi.org/10.3390/info12120529

Academic Editor: Willy Susilo

Received: 30 October 2021
Accepted: 8 December 2021
Published: 20 December 2021

1. Introduction

Due to the enhanced global interconnection of massive computer networks, the internet is now accessible to about 70% of the world's population [1]. In the years to come, this percentage is expected to increase because giant technological companies such as Amazon, SpaceX, and Virgin Galactic are investing heavily in research and development efforts that will ultimately guarantee ubiquitous access to the internet [2,3]. Today, typical end-user devices such as mobile devices (e.g., phones, tablets, and others), personal computers, and others constitute part of larger networks whose interconnections have been made possible by the internet [4]. This global infrastructure, which primarily enables the connection of all kinds of devices to allow for augmented or enhanced wireless communications and the sharing of information between devices, is generally referred to as the Internet of Things (IoT) [5].

Apart from the robust wireless connectivity of devices, the IoT also allows for remote or virtual human-to-human, human-to-machine, and machine-to-machine interactions [6–8]. These and many other capabilities (such as pervasiveness or ubiquity) of the IoT are what makes it attractive for many specialised applications such as process monitoring and control across many industries, which has led to the advent of the Industrial IoT (IIoT) [5,9]. While IIoT and its applications in and of themselves are not posited to usurp or replace existing industrial systems such as legacy automation and manufacturing systems [10], IIoT paradigms are bound to offer expedited means of ensuring smart monitoring and intelligent control of these systems for improved productivity and reliability [11]. A case in point attracting a great deal of interest is the full decentralisation or quasi-decentralisation of the control architectures of traditional industrial control systems (ICSs) enabled by multiple agents that are connected by the internet and act alongside industrial control units (ICUs) to support the ubiquitous control and/or monitoring of industrial systems [12–14].

To develop a human–machine interface (HMI) for the ubiquitous control of industrial machines and equipment as a paradigm for IIoT applications, the control units or systems for industrial machines such as computer numerical control (CNC) machines must firstly have a dedicated connection to a standard industrial data network such as process field net (PROFINET) [15]. Because programmable logic controllers (PLCs) (the dedicated control units for most industrial machines and equipment) are designed to have network ports that are compatible with the transmission control protocol and internet protocol (TCP/IP) suite, it is possible to make a PLC-based industrial machine or equipment a node on a larger network such as the internet. To implement this, the primary challenge is to have a device that routes signals between the machine's PROFINET (localised industrial network of the machine without internet connection) and the Ethernet (local area network for internet connectivity). Additionally, purpose-built technologies such as single-board multipurpose computers with on-board micro-controller units (e.g., Raspberry Pi [16]) will be required for the transmission of digital signals from the HMI (now made ubiquitous over TCP/IP) to the control unit of the machine over TCP/IP. This sort of control architecture poses another challenge in terms of cybersecurity. This is because the industrial machine and its peripherals go online over TCP/IP, making the industrial system in effect a cyber-physical system (CPS) [17,18]. Furthermore, since the ubiquitous HMI is expected to be portable and mobile, a handheld device with a very low profile in terms of size and weight and an override system (i.e., emergency buttons) that can be easily accessible by system operators' fingers to ensure speedy interventions are required.

In this work, a handheld lightweight integrated system is proposed as a proof of concept (PoC) for the ubiquitous control of industrial machines to overcome the challenges and meet the functional requirements described above. The proposed PoC offers the following features which are in accordance with state-of-the-art paradigms for the remote, quasi-decentralised and pervasive control of industrial machines and equipment in line with present-day IIoT trends:

- Display of the states of the industrial machine via a web-based ubiquitous HMI, making the industrial system in effect a CPS;
- Multi-factor authentication including an administrative password and the IP address of the industrial machine to control access to the web-based ubiquitous HMI of the proposed PoC, to avert potential cyber attacks or threats that are often associated with wireless communication systems such as IIoT systems;
- Touchscreen-based input configurations to manage control actions on the industrial machine over TCP/IP for the remote, quasi-decentralised and ubiquitous control of the industrial machine through the use of multiple agents (a Samsung Galaxy Tablet S2 and a Raspberry Pi 4), acting alongside the traditional PLC-based ICU;
- Conventional override system achieved with emergency and acknowledge actions on the industrial machine via digital signals from push buttons implemented over TCP/IP for the more robust, remote, quasi-decentralised, and ubiquitous control of the industrial machine through the use of multiple agents (a Samsung Galaxy Tablet S2 and a Raspberry Pi 4), acting alongside the traditional PLC-based ICU.

The remainder of the paper is organised as follows: Section 2 summarily discusses the related work to reemphasise the practical needs of the work carried out; Section 3 describes the adopted devices and systems for the implementation of the PoC; Section 4 details the modi operandi of the working prototype of the PoC, including the configurations and operations of the adopted devices, and a performance evaluation of the PoC; Section 5 highlights the challenges and limitations of the working prototype of the PoC; and the concluding remarks are provided in Section 6.

2. Related Work

Due to new intelligent and innovative operations such as remote configuration, self-diagnosis, etc., present-day industrial production and manufacturing processes demand highly robust operations and the quasi or full decentralisation of the control architectures for the integrated and distributed control of the machines and equipment deployed on the shop floor [12,19,20]. The extent of decentralisation will always be relative to the architecture or arrangement of the ICSs and the coupling between the subsystems that make up the ICSs. Robust operations (e.g., pervasive sensing for time-critical applications [21]), guaranteed functional safety of electrical drives and machines (e.g., forced shutdown or emergency stop of industrial machines in line with global standards and practice [22]), and improved energy efficiency (e.g., energy-efficient or optimum pump operations in cooling systems [23]) can often be realised on ICSs through the use of mobile or ubiquitous HMIs acting as multiple agents or add-ons or complementary platforms alongside traditional ICUs (typically, PLCs) [7,24]. Depending on their arrangement and operations, these ubiquitous HMIs allow for the quasi or full decentralisation of the control architectures of traditional ICSs.

The quasi or full decentralisation of the control architectures of traditional ICs is required because the conventional centralised control architecture, which overly relies on a single agent or component (usually, a PLC) to be the designated controller, does not always support the management of information structure constraints, uncertainties, delays, and a large span of control in the physical absence of a system operator on the shop floor [20]. Present-day high dimensional large-scale complex industrial systems often require robust remote operations in the absence of a system operator on the shop floor [25,26]. As a result, fully decentralised and quasi-decentralised control architectures offer the advantages of ease of expansion of the ICS, better localisation of faults, better supervision and control, and more robustness in comparison to conventional fully centralised control architectures [13,14,25–27].

In [24], to make industrial process visualisation and supervisory plant process monitoring process more decentralised, flexible and robust, non-conventional HMIs (power-wall and table) are proposed and investigated using an experimental agent-based HMI for supervisory control and data acquisition (SCADA). In principle, the paradigms in [24] can conveniently be adopted to design and develop ubiquitous or online SCADA systems for industrial applications. However, to ensure the mobility of the remote control architecture, the physical dimensions of the HMIs and the overall remote control architecture in [24] could be challenging to implement on a small scale with a low profile.

To demonstrate the feasibility of employing mobile HMIs for the decentralisation and ubiquity of ICSs, a framework that allows for the open-source design and development of native mobile Android-based HMIs for ICSs is proposed in [7]. The methodology is demonstrated via successful home automation, sewage treatment plant, and traffic lights control system case studies. Even though these case studies circumvent the cost overhead associated with proprietary solutions [28] (e.g., MobileHMI [29]), actual sensors have not been connected to the PLCs in the implementation as expected in real practice. Additionally, the implementation also requires a number of ad-hoc processes such as the generation, verification and execution of the Android code.

To support IIoT paradigms that enable the digitisation of the shop floor and subsequent decentralisation of the control architectures for ICSs, today, many leading manufacturers of industrial automation and control products offer products that provide the flexibility of innovative user-end design and development of mobile HMIs on a number of mobile operating systems [30,31]. Siemens AG tends to be at the forefront of this, with award-winning products such as their range of Simatic PLCs [32,33]. Specifically, in [34], an IIoT paradigm for the control of industrial machines is presented in which the Simatic HMI comfort panel designated for operating industrial machines can be accessed remotely by a standard computer through a virtual private network (VPN).

Such a VPN can be leveraged to implement low-cost, low-profile mobile HMIs by simply making the VPN accessible on compatible handheld or mobile devices over TCP/IP. Even though such mobile or ubiquitous HMIs will adequately support the quasi or full decentralisation of the control architectures of their associated ICs, as discussed above, they also make their ICSs prone to cyber attacks or threats due to their dedicated internet connectivity [35]. Several frameworks and/or methodologies such as the National Institute of Standards and Technology (NIST) framework [36,37] are available today to assess cyber attacks or threats such as denial of service [38] and devise the means of mitigating them in industrial applications, but cybersecurity has remained an area of ongoing research due to its very broad and dynamic nature in industrial applications [39].

In this work, a low-cost and low profile quasi-decentralisation of the conventional PLC-based control architecture for a state-of-the-art CNC machine (Studer S33) is achieved through data and information exchange between multiple agents (a Samsung Galaxy Tablet S2 and a Raspberry Pi 4) and the dedicated ICU (Siemens Simatic S7-1200) of the CNC machine over TCP/IP. The quasi-decentralisation achieved adequately supported the ubiquitous control of the CNC machine through the configuration of the first agent (Raspberry Pi 4) as a dedicated wireless access point (WAP) on the control architecture of the investigated ICS. In this way, the additional agent (Samsung Galaxy Tablet S2) is made an actor within the control architecture of the investigated ICS via a web-based application. Consequently, the quasi-decentralisation made the investigated ICS in effect a CPS. Since the proposed PoC causes the ICS to double as a CPS, the primary gateways for potential cyber attacks or threats are identified to be the WAP configured on the first agent (Raspberry Pi 4) and the web-based application configured on the second agent (Samsung Galaxy Tablet S2).

Following the recommendations in [40], a multi-factor authentication (administrative password and IP address) is adopted in this work to prevent the web-based application on the Samsung Galaxy Tablet S2 from unauthorised access and transferring sensitive information. To secure the Raspberry Pi 4 from potential cyber attacks or threats, the default username and password of its operating system (OS) were changed to a more secure username and password comprising alphanumeric and symbols as recommended in [41]. In addition, the port of the secure shell protocol (SSH) on the OS of the Raspberry Pi 4, which allows for remote log on, was closed to ensure that it cannot be accessed remotely for reconfiguration as suggested in [41].

In comparison to some of the recent works discussed above, the proposed PoC is relatively secure, and it offers a higher degree of simplicity in terms of configurations and affordability (considering development and operational costs), while achieving a quasi-decentralisation of the control architecture of the investigated ICS to allow for the ubiquity of control operations. In the subsequent sections, the proposed PoC and its features are discussed to reveal how it might support the development of full-fledged systems for the full decentralisation of the control architectures of traditional ICSs in line with contemporary IIoT paradigms.

3. Adopted Devices and Systems

The layout of the proposed PoC is shown in Figure 1. In Figure 1, the essential devices and systems that constitute the proposed PoC are a tablet with HMI (Samsung Galaxy Tablet S2 [42]), a PROFINET slave/device (Raspberry Pi 4 [16,43]), an Ethernet switch (Netgear GS305E switch [44]), and a PROFINET master, a PLC (Siemens Simatic S7-1200 [45,46]) integrated with a state-of-the-art CNC universal cylindrical grinding machine (Studer S33 [47]). As shown in Figure 1, all the devices and systems are connected to each other via physical cables, except the tablet with HMI, which bidirectionally communicates with the PROFINET Slave/Device using a wireless internet link (i.e., over the TCP/IP). Note that the link between the PROFINET Slave (Raspberry Pi 4) and the Ethernet switch (Netgear 305E) could be implemented using a physical cable (an Ethernet cable) or a wireless medium (Wi-Fi access point). It is essential to have a wireless connection between the PROFINET Slave and the Ethernet switch to demonstrate the full extent of the ubiquity of the control mechanism the proposed PoC offers. In practice, the tablet with HMI is to be collocated with the PROFINET slave to support physical connections to external compatible modules for sensing and actuation .

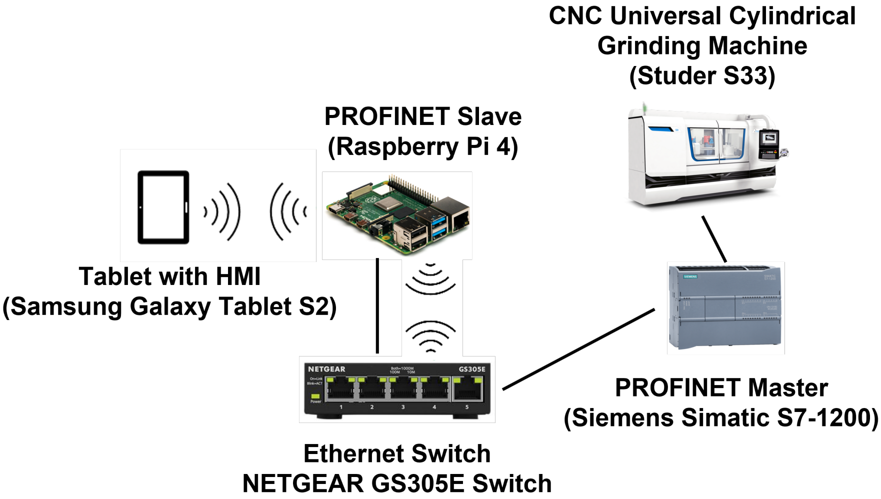
CNC Universal Cylindrical Grinding Machine (Studer S33)
PROFINET Slave (Raspberry Pi 4)
Tablet with HMI (Samsung Galaxy Tablet S2)
PROFINET Master (Siemens Simatic S7-1200)
Ethernet Switch NETGEAR GS305E Switch

Figure 1. Layout of the proposed PoC showing the adopted devices and systems.

The devices and systems that constitute the proposed PoC are summarily described as follows to highlight their specific functions.

3.1. CNC Machine

The industrial machine to be controlled in the proposed PoC is a CNC universal cylindrical grinding machine (Studer S33) [47]. The Studer S33 is a state-of-the-art industrial CNC machine designed to cut different sizes of medium workpieces at a cutting speed of up to 50 ms^{-1}. It can be equipped with different grinding tools, and it supports both individual and batch production of medium-sized workpieces. Using purpose-built application software (StuderPictogramming and StuderWINgramming), the grinding process on the Studer S33 can be configured or programmed either using the HMI of its relatively portable control unit (Fanuc 0i-TF [48]) or a personal computer (PC) linked to its control unit. A constant cutting speed can be configured for the Studer S33 using a turret wheelhead with a frequency-controlled motor spindle. More technical details about the S33 can be found in [47].

3.2. PROFINET Master

The PROFINET master in the proposed PoC is the Siemens Simatic S7-1200 [45,46], as shown in Figure 1. It is a device that provides the required degree of flexibility and power to control a wide variety of industrial machines such as CNC machines. It has a compact design, robust instruction set, and flexible configuration to support many industrial applications. Its central processing unit (CPU) comprises a microprocessor, an integrated power supply, input and output circuits (I/Os), built-in PROFINET, high-speed motion control I/O, and on-board analog inputs. Due to its flexibility and robustness, the Siemens Simatic S7-1200 can effectively and efficiently control large machines such as robot manipulators using complex and dynamic programming cycles. Additionally, its I/Os can all be employed at the same time by adding additional units, in which each has about

20 inputs and 20 outputs. The central processing unit (CPU) of the Siemens Simatic S7-1200 provides a PROFINET port for communication over a PROFINET network. Additional modules are also available for communicating over the process field bus (PROFIBUS), RS485 and RS232 networks, and Ethernet networks. In this way, the Siemens Simatic S7-1200 can link PROFINET and Ethernet devices together and be programmed to send specific commands to an IP address such that nodes on the network can control and/or read the I/Os. More technical details about the Siemens Simatic S7-1200 can be found in [45,46].

3.3. Ethernet Switch

To link the devices and systems in the proposed PoC, as shown in Figure 1, Ethernet cables with RJ45 connectors and an Ethernet switch are required. The Ethernet switch adopted in the proposed PoC is the Netgear 305E switch [44]. Note that other Ethernet switches (including Ethernet switches that have an integrated Wi-Fi (wireless fidelity) access point) can be used. The Netgear GS305E switch has a buffer size of 128 kB, a performance bandwidth of 10 Gps, and a meantime between failure of 2,531,294 h at 25 °C. It operates using the IEEE 802.1p class of service (COS) and a port-based virtual local area network (VLAN). With its integrated VLAN function, the Netgear GS305E switch supports the configuration and establishment of different networks. More technical details about the Netgear GS305E switch can be found in [44].

3.4. PROFINET Slave

The PROFINET slave or device in the proposed PoC is the Raspberry Pi 4, as shown in Figure 1. The Raspberry Pi 4 is basically is a single-board computer using a Linux operating system. The Raspberry Pi 4 can be deployed as a computer with a graphical user interface (GUI). Even though the Raspberry Pi 4 is not as powerful and robust as the better-known personal computers with more computational power and capabilities, it is capable of carrying out several computational and processing tasks. It comes with an Ethernet port and a Wi-Fi module to allow for network connectivity, and it has digital I/Os that are compatible with analogue-to-digital converter chips. In this way, the Raspberry Pi 4 is capable of working with analogue data or signals. Due to this functionality, push buttons and industrial machines such as motors can be connected to the Raspberry Pi [16]. For wireless connectivity, the Raspberry Pi 4 uses a dual-band IEEE 802.11b/g/n/ac wireless that can run at 2.4 GHz (licensed industrial, scientific and medical (ISM) band) or 5.0 GHz (Unlicensed National Information Infrastructure (U-NII) band) [49]. More technical details about the Raspberry Pi 4 can be found in [43,49].

3.5. Tablet with HMI

The proposed PoC uses the Samsung Galaxy Tablet S2 as its tablet with HMI, as shown in Figure 1. The Samsung Galaxy Tablet S2 has a multi-touch touchscreen and an on-board Wi-Fi module that supports the IEEE 802.11 a/b/g/n/ac wireless networking standards, allowing for dual-band connectivity, 2.4 GHz or 5 GHz, similar to the Raspberry Pi. Since several Android OS-based applications such as internet browsers can also be installed, configured, and deployed on the Samsung Galaxy Tablet S2, it is highly compatible for the deployment of HMIs [50]. These features are harnessed to have a web-based HMI on the Samsung Galaxy Tablet S2 for the proposed PoC as shown Figure 2. More technical details about the Samsung Galaxy Tablet S2 can be found in [42].

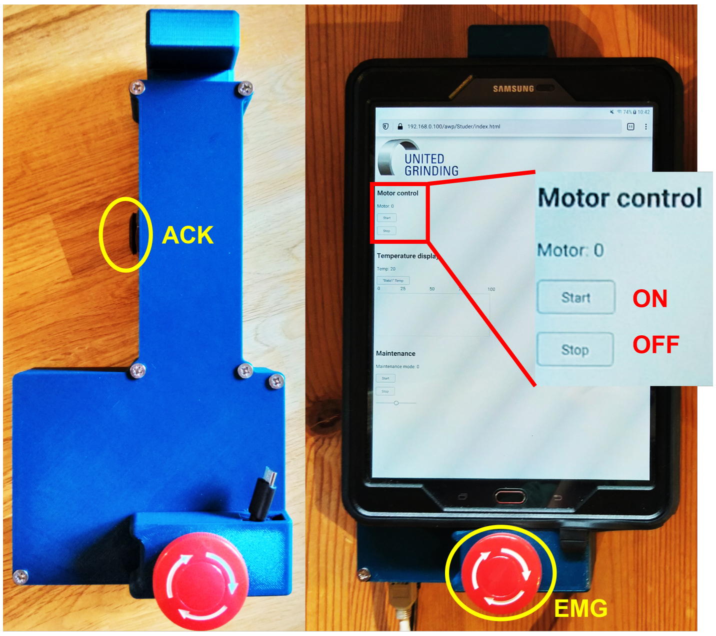

Figure 2. Tablet with HMI for controlling the CNC machine for the proposed PoC.

4. The Proposed PoC

The primary function of the CNC universal cylindrical grinding machine (Studer S33) used for the PoC is to grind metallic pieces mounted to a spindle. The spindle and a collaborative robot arm operating the grinding tool are controlled by a PLC (Siemens Simatic S7-1200 PLC in this case) and programmed to allow the movement and rotation of workpieces in different angles. In this way, the collaborative robot arm can drill at different velocity rates. When used cooperatively with the rotating spindle, the Studer S33 can be configured to grind various workpieces via an external control panel. The Samsung Galaxy Tablet S2 (Tablet with HMI) is configured to be the "control panel" for the PLC using PROFINET. Hence, Siemens Simatic S7-1200 PLC is the PROFINET master as described in Section 3.2. To access the Siemens Simatic S7-1200 PLC over PROFINET using the Samsung Galaxy Tablet S2, the PROFINET master is set up with a fixed IP address. By activating the web-server function of the PROFINET master and creating a website in HTML (HyperText Markup Language), a web-based HMI for the PROFINET master becomes accessible over TCP/IP from any device with a browser that fulfills the MFA (IP address and administrative password) as shown in Figure 3. In this way, connected devices automatically become part of the industrial network after fulfililng the MFA.

The web-based HMI is configured to send commands to the main programming logic that initiates the control operation sequences on the Studer S33. The conventional HMI for the CNC universal cylindrical grinding machine (S33) is the control unit (Fanuc 0i-TF [48]) as mentioned in Section 3.1. It is attached over a movable arm and has a size of about 1000 mm by 60 mm. These features indicate that the conventional panel is not very compact, and it is fixed at the location of the CNC machine. To program and configure the control unit of the CNC, a personal computer (PC) is first connected to the PROFINET master. The Siemens Totally Integrated Automation (TIA) Portal is used to both configure and program the PROFINET master. Since the TIA Portal is not designed to directly control the CNC machine, attempting to do so seems impractical; hence, in the proposed PoC, it is the PROFINET master (Siemens Simatic S7-1200) that is linked to the network used for the ubiquitous control of the Studer S33 and not the PC used to configure and program it.

4.1. Configuration

As mentioned in Section 3, a Samsung Galaxy Tablet S2 is linked to the Siemens Simatic S7-1200 PLC over PROFINET. This is done by configuring a Raspberry Pi 4 as a router to function as a dynamic host configuration protocol (DHCP) server and wireless access point (WAP) using a dual-band (2.4 GHz (ISM band) or 5.0 GHz (U-NII band)) Wi-Fi. By connecting both devices to the Raspberry Pi 4, a TCP/IP connection is established. The PROFINET master is configured according to Listing 1 and the Raspberry Pi 4 is configured according to Listing 2.

Listing 1. Configuration of the PROFINET master (Siemens Simatic S7-1200).

```
Begin
Open Siemens TIA portal
Create a new project to configure Siemens Simatic S7-1200
Select device type = Hardware type
Open the “General Settings”
    In “PROFINET Interface”
      Set the “IP Address” and “Subnet Mask” to according to the network
        Under “Advanced Options”
          Activate “Web Server Access”
        Under “Protection and Security”
          Activate the PUT/GET Option
    In “Pulse Generators (PTO/PWM)”
      Set “Startup after POWER ON” to “Warm Restart-RUN”
    In “Web Server”
      Create a new user and grant full access
        If (Device == Offline) Then
          Click “Go online” and “Start search”
        End
        If (Device == Found) Then
          Double click the device
        End
End
```

4.2. Operations

The flow diagram of the operations of the proposed PoC is shown in Figure 3, and the communication system layout is shown in Figure 4. The essential steps are described summarily as follows:

- **Step 1:** To control the CNC universal cylindrical grinding machine (Studer S33) ubiquitously, the system operator makes use of the touchscreen-operated Tablet (see Figure 3). By using a browser application, installed and configured on the tablet, the system operator enters the IP address of the CNC machine, and the web-based HMI created for the PROFINET master (Siemens Simatic S7-1200) can be accessed using an administrative password (see Figure 3).
- **Step 2:** Following a successful authentication in Step 1, full administrative access is granted to the web-based HMI. Using the touchscreen of the tablet, the user can perform the following operations on the industrial motor: (1) ON (2) OFF (3) ACK (Acknowledge) (4) EMG (Emergency), as shown in the communication system layout in Figure 4.
- **Step 3:** Depending on the system operator’s selection in Step 2, while the ACK button is pressed down, the Studer S33 is “started” for ON or “stopped” for OFF. To “shut down/stop” the Studer S33 immediately, the EMG button shown in Figure 4 can used at any time.
- **Step 4:** Once the Studer S33 is configured in Step 3, it remains in the configured state, and the entire process reiterates back to Step 1.

Listing 2. Configuration of the PROFINET slave (Raspberry Pi 4).

```
Begin
Configure the LAN connection of Raspberry Pi 4
Use a fixed IP-address in the file “/etc/dhcp.conf”
In the same file (i.e., “/etc/dhcp.conf”)
    Prioritize WLAN connection over LAN connection
Activate the general-purpose I/Os (GPIOs)
In the command line
    Implement “sudo apt-get update
      To request updates for Raspberry Pi 4
    Implement “sudo apt-get install python-rpi.gpio”
      To insall python-rpi.gpio
    Implement “sudo adduser $USER gpio”
      To add user (“USER”) to the group for the GPIOs
In the command line
    Implement “sudo apt install hostapd”
      To installaccess point software package
At the startup (booting) of the Raspberry Pi 4
    Implement “sudo systemctl unmask hostapd”
    And      Implement “sudo systemctl enable hostapd”
      To enable and start access point
    Implement “sudo apt install dnsmasq“
      To install the package for domain name system (DNS) and DHCP
        DHCP - distribute IP addresses to the connected devices
        DNS service - translate domain name of devices to IP addresses
    Implement “sudo DEBIAN_FRONTEND = noninteractive apt ...
    install -y netfilter-persistent iptables-persistent”
    And      Implement “sudo iptables -t nat -A POSTROUTING ...
    -o eth0 -j MASQUERADE“
      To add firewall rules for data traffic sharinf between the devices
    Implement “sudo apt-get install netfilter-persistent -y”
      To install the service iptables-persistent to save firewall rules
    Implement “sudo netfilter-persistent save”
      To save firewall rules
Add a static IP-address for “wlan0” in the file “/etc/dhcp.conf”
In the command line
    Implement “sudo nano /etc/sysctl.d/routed-ap.conf”
      To enable the routing between ethernet and WiFi
Add the text “dnsmasq.conf” to the newly created file
    To enable the routing by setting the configuration for the DHCP service
Rename the original file
In the command line
    Implement “sudo mv/etc/dnsmasq.conf /etc/dnsmasq.conf.orig”
    And      Implement “sudo nano/etc/dnsmasq.conf”
      To have connected devices with IP addresses in the defined DHCP range
    Implement “sudo rfkill unblock wlan”
      To unblock WiFi
    Implement “sudo nano/etc/hostapd/hostapd.conf”
      To create a new file to configure Wi-Fi
        Define Wi-Fi service set identifier (SSID), password and others
Reboot Device to connect and make access point go live
Connect tablet to both Wi-Fi and Raspberry Pi 4
Access the website of the PROFINET master
End
```

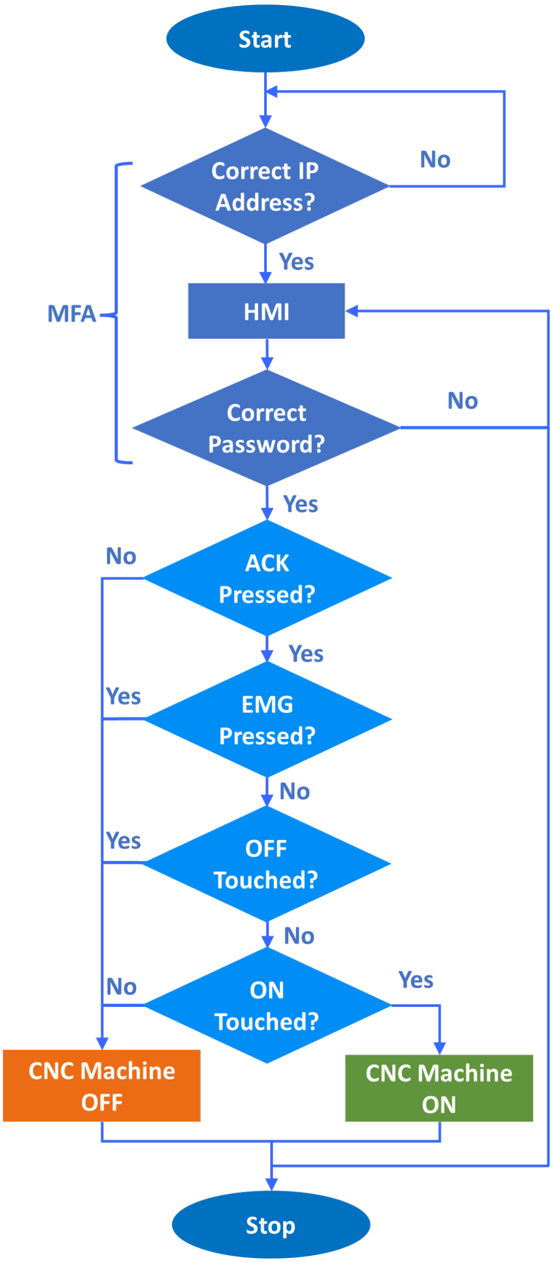

Figure 3. Flow diagram of the operations of the proposed PoC.

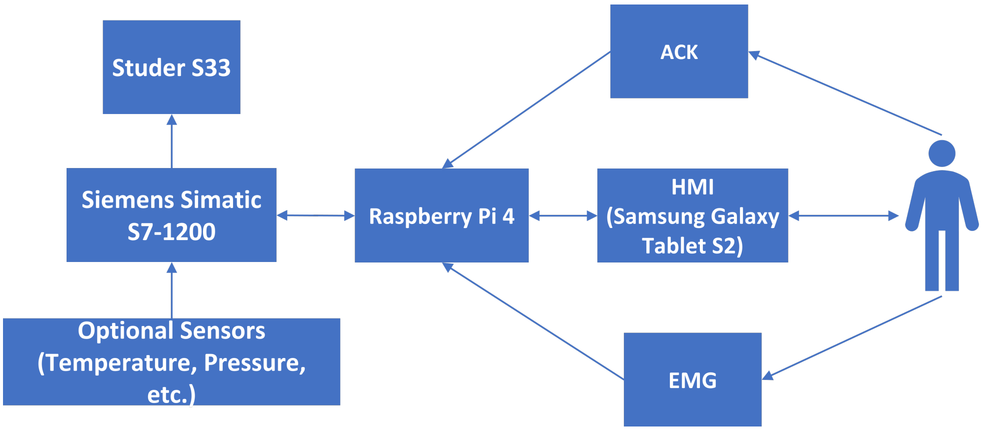
Studer S33
Siemens Simatic S7-1200
Optional Sensors (Temperature, Pressure, etc.)
Raspberry Pi 4
ACK
HMI (Samsung Galaxy Tablet S2)
EMG

Figure 4. Communication system layout of the proposed PoC.

4.3. Analysis and Performance Evaluation

To analyze the operations of the proposed PoC and to evaluate its performance, its control operations must firstly be modelled mathematically to determine the best metric or set of metrics to adopt or employ. In this work, the control operations of proposed PoC can be modelled to address a minimum-time control problem [51], considering the state switching procedure of the Studer S33 (i.e., State 0: OFF $\Longleftrightarrow$ State 1: ON, as shown in Figure 5) effected by the proposed PoC. Note that a full-fledged system should accommodate more states in the state switching procedure of the Studer S33; for example, the downtime, standby, idle, warm up, and operational states in the typical state switching procedure of a CNC machine tool [52]. However, these states are not within the scope of our work due to the control operations configured on the proposed PoC. As a result, all states of the Studer S33 are concatenated into two main states (i.e., ON and OFF states) to reflect the primary operations offered by the proposed PoC (see Figure 5). It is envisaged that these two states are sufficient to support the investigative studies carried out in this work to guide the potential development of a full-fledged system that can take into account several states of the Studer S33.

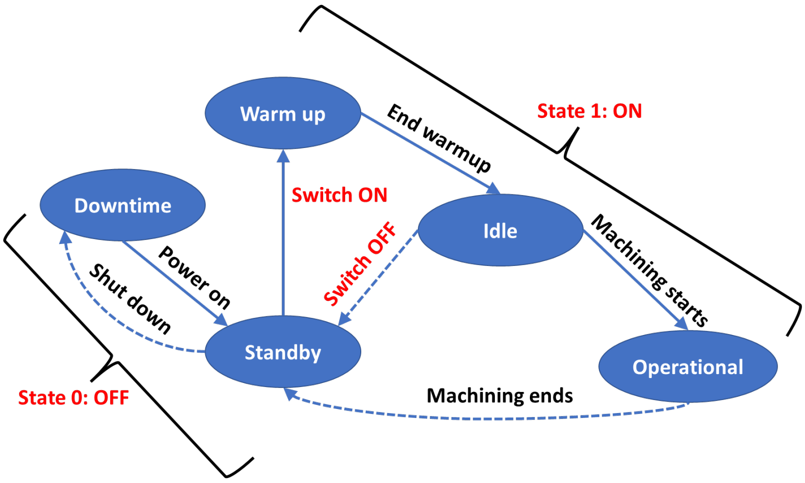

Figure 5. Concatenation of the state switching procedure of the CNC machine.

Using the two states of the Studer S33 that can be controlled by the proposed PoC, intuitively, it can be deduced that the control mechanism offered by the proposed PoC mirrors the conventional bang–bang controller that is often implemented for industrial machines that accept or can be configured to accept binary inputs such as the opening and closing of a switch [53]. To model the bang–bang control signal (i.e., ON or OFF signal) from the proposed PoC, a formulation of the Heaviside step function can be used as follows:

$$H[t] = \begin{cases} 0 \text{ (OFF State)}; \forall t = t_{OFF} \\ 1 \text{ (ON State)}; \forall t = t_{ON} \end{cases} \tag{1}$$

where t_{OFF} and t_{ON} are all the instances of time for which the Studer S33 is activated ON and OFF, respectively, by the proposed PoC, as shown in Figure 6. This follows from the assumption made that the Studer S33 remains in an OFF state for all instances of time until it receives an ON state signal from the proposed PoC or vice versa (see Figure 5).

To better understand the formulation in Equation (1), the latency (t_L) of the proposed PoC can be said to be directly proportional to the dead time (t_D) of its bang–bang control scheme. This is because the time taken for the proposed PoC to transfer data (i.e., ON or OFF activation signal) from the Samsung Galaxy Tablet S2 (i.e., tablet with HMI) to Studer S33—i.e., t_L—will always be directly proportional to the delay from when the bang–bang control signal is issued until when the Studer S33 responds to the control signal; i.e., t_D. This relationship can be expressed as follows:

$$t_L \propto k \times t_D \tag{2}$$

where k is the proportionality constant, which is assumed to be unity in our investigations for simplicity. This assumption is made because the individual time frames for t_L and t_D cannot be correctly ascertained to be distinguishable without rigorous analysis and investigations that are beyond the scope of this work. Hence, $t_L = t_D$ is used in the subsequent investigations.

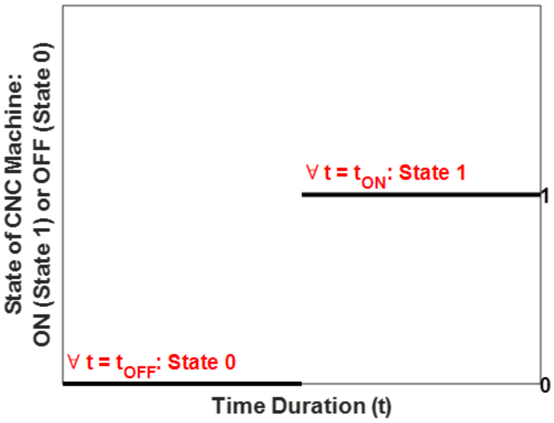

Figure 6. Mathematical model of the operations of the proposed PoC.

For the typical operation of the Studer S33 using the proposed PoC (i.e., initialisation from $t = 0$, as the initial period), if the Studer S33 is initially in an OFF state (i.e., State = 0) based on the condition $\forall\ t = t_{OFF}$ and it is expected to be in the ON state (i.e., State = 1) based on the condition $\forall\ t \neq t_{OFF}$, this cycle of operation can be modelled mathematically as shown in Figure 7. The plot of the mathematical model shown in Figure 7 can be described analytically as follows:

$$[H(t - t_D) - H(t - (t_{ON} + t_D))] \tag{3}$$

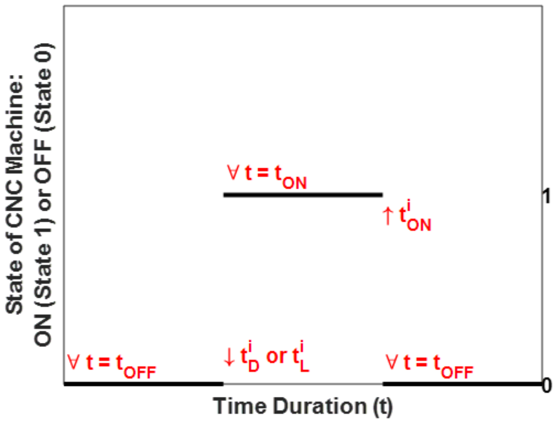

Figure 7. Mathematical model of the operations of proposed PoC for an operational cycle (ith cycle) of the CNC machine.

If t_{OFF} is $\forall\ t \neq t_{ON}$, by considering, t_{OFF}, t_{ON} and $t_L = t_D$, the Heaviside step function formulation for the bang–bang control scheme offered by the proposed PoC can be modelled mathematically, more accurately, as follows, for an ith operational cycle of the Studer S33:

$$[H(t - t_D^i) - H(t - (t_{ON}^i + t_D^i))] = \begin{cases} 0 \text{ (OFF State)}; t < t_D^i \\ 1 \text{ (ON State)}; t_D^i \leq t < t_D^i + t_{ON}^i \\ 0 \text{ (OFF State)}; t \geq t_D^i + t_{ON}^i \end{cases} \tag{4}$$

where $t_D^i = t_L^i$.

From Equation (4) and Figure 7, it can be seen that t_D or t_L is a very important metric for the evaluation of the performance of the proposed PoC with respect to the operational cycles of the Studer S33. In this work, we have analysed the t_D or t_L of the proposed PoC over 100 operational cycles of the Studer S33 to ascertain the performance of the proposed PoC. The descriptive statistical analysis carried out is shown in Table 1 and the trends for the OFF and ON control states over the operational cycles are shown in Figure 8.

From Table 1, it can seen that over 100 operational testing cycles of of the CNC machine (Studer S33), the mean values of t_D or t_L for the OFF and ON activation states (i.e., 0.8040 s and 0.7919 s, respectively) are in close agreement and reasonably match the standard conventions for bang–bang control schemes designated for the control of physical systems [54]. In addition, the worst values of t_D or t_L for the OFF and ON activation states (i.e., 0.9300 s and 0.9500 s, respectively) are still relatively fast. This shows that the proposed PoC is still efficient, even for the worst-case scenario. A low standard deviation of the t_D or t_L values for the OFF and ON activation states over the operational testing cycles—i.e., 0.0613 and 0.0656, respectively—indicates that the proposed PoC offers a very robust t_D or t_L. This is further corroborated by the trends in Figure 8. In Figure 8, it can be seen that t_D or t_L is relatively stable for the OFF and ON activation states over the operational testing cycles of the CNC machine (Studer S33).

Table 1. Performance evaluation of the proposed PoC in terms of t_D or t_L in seconds over 100 operational testing cycles.

Operational Mode or Activation State	Best (t_D or t_L)	Worst (t_D or t_L)	Mean (t_D or t_L)	Standard Deviation
OFF State (0)	0.6300	0.9300	0.8040	0.0656
ON State (1)	0.6100	0.9500	0.7919	0.0613

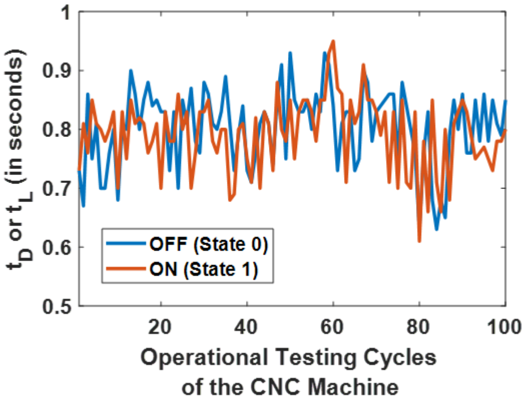

Figure 8. t_D or t_L trends for the OFF and ON states of the CNC machine over 100 operational testing cycles.

5. Challenges and Opportunities

Using the tablet with HMI (i.e., web-based HMI), the CNC machine can be started or stopped. In addition, a maintenance mode can be turned ON or OFF, during which the acknowledge button (i.e., ACK in Step 3 in Section 4) needs to be pressed down for safety reasons. The emergency stop button (i.e., EMG in Step 3 in Section 4) is used to halt the running processes on the Studer S33 immediately in case of an emergency. To provide further control of the Studer S33, the web-based HMI can be programmed to manage hole grinding processes and display the status of running tasks and additional operational states of the CNC machine. Additional sensors and their readings can also be incorporated on the shop floor to provide status updates and other alerts, as depicted in Figure 4), to other connected devices (e.g., other portable devices) on the network. In this way, the connected devices can access and manage the Studer S33 and its operations on the shop floor from anywhere on the globe. In other words, the PoC effectively portrays a CPS—one of the core components of the IIoT.

Despite the ubiquitous control and robust digital footprints that the PoC affords the CNC machine (Studer S33), an "online" presence means that the machine can be accessed and controlled once the administrative and other access control measures such as a firewall have been bypassed. As a standard configuration on the PROFINET master (Simatic S7-1200), MFA including an administrative password with the IP address of the Studer S33 is set to access the web-based HMI. In this way, even though the machine is "online", only authorised users can connect to the PLC's main control website and are able to access the web-based HMI based on the MFA, as shown in Figure 3. More factors such as key generation in the form of verification codes or one-time passwords (OTPs) sent to the operator via email or short message service can also be incorporated into the MFA as additional layers of access control to the web-based HMI to further alleviate potential cyber attacks or threats.

Due to the inherent constraints of web-based applications, programs for purpose-built web applications are often limited to compatible development languages. Hence, the level of interactivity of web-based HMIs could be limited as well because of the inherent constraints in programming constructs. Since the proposed PoC works over TCP/IP, the bandwidth and connection speed of the internet may also impose a t_L that compounds the t_D associated with controlling the CNC machine (Studer S33) via the web-based HMI.

6. Conclusions

To demonstrate the ubiquitous and wireless control of industrial machines, a PoC comprising a state-of-the-art CNC machine (Studer S33), a PLC (Siemens Simatic-1200), an Ethernet switch (Netgear 305E), a single-board computer (Raspberry Pi 4), and a commercially available tablet (Samsung Galaxy Tablet S2) is developed and investigated in this work as an IIoT paradigm. The ubiquitous and wireless control (primarily, ON and OFF operations) of the Studer S33 achieved via a web-based HMI on the Samsung Galaxy Tablet S2 validates the prospective use of the PoC in IIoT applications involving industrial machines on the shop floor. The profile, weight, and size of the working prototype of the mobile (handheld) touch-sensitive HMI, which fits into a 300 mm by 180 mm by 175 mm compact case, also demonstrates the enhanced mobility and ubiquity that the PoC offers in comparison to conventional or traditional industrial control units. In the future, the integration of sensors and sensing paradigms into the network to pervasively monitor processes and operations on the shop floor will be investigated using the PoC and findings in this work as a backbone for the development of a full-fledged system.

Author Contributions: Conceptualization, S.A.A. and M.O.A.; methodology, S.A.A., M.O.A., S.M. and M.L.J.; software, S.A.A.; validation, M.O.A.; formal analysis, M.O.A.; investigation, S.A.A.; resources, S.A.A. and M.O.A.; data curation, S.A.A. and M.O.A.; writing—original draft preparation, S.A.A. and M.O.A; writing—review and editing, S.A.A., M.O.A., S.M. and M.L.J.; visualization, S.A.A. and M.O.A.; supervision, M.O.A., S.M. and M.L.J.; project administration, M.O.A.; funding acquisition, M.O.A. All authors have read and agreed to the published version of the manuscript.

Funding: The APC for this work was supported in part by the Faculty of Arts, Science and Technology, Wrexham Glyndŵr University, U.K.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to sincerely thank Fritz Studer AG for providing the equipment for the design, development and testing of the proposed PoC.

Conflicts of Interest: The authors declare no conflict of interest. The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Mulaydinov, F. Digital Economy Is a Guarantee of Government and Society Development. *Ilkogr. Online* **2021**, *20*, 1474–1479.
2. Foust, J. Spacex's space-internet woes: Despite technical glitches, the company plans to launch the first of nearly 12,000 satellites in 2019. *IEEE Spectr.* **2018**, *56*, 50–51. [CrossRef]
3. McDowell, J.C. The low earth orbit satellite population and impacts of the SpaceX Starlink constellation. *Astrophys. J. Lett.* **2020**, *892*, L36. [CrossRef]
4. Gralla, P. *How the Internet Works*; Que Publishing: Upper Saddle River, NJ, USA, 1998.
5. Weber, R.H.; Weber, R. *Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 12.
6. Wood, A.F.; Smith, M.J. *Online Communication: Linking Technology, Identity, & Culture*; Routledge: London, UK, 2004.
7. Qasim, I.; Anwar, M.W.; Azam, F.; Tufail, H.; Butt, W.H.; Zafar, M.N. A model-driven mobile HMI framework (MMHF) for industrial control systems. *IEEE Access* **2020**, *8*, 10827–10846. [CrossRef]
8. Misic, V.B.; Misic, J. *Machine-to-Machine Communications: Architectures, Technology, Standards, and Applications*; CRC Press: Boca Raton, FL, USA, 2014.
9. Koulamas, C.; Kalogeras, A. Cyber-physical systems and digital twins in the industrial internet of things [cyber-physical systems]. *Computer* **2018**, *51*, 95–98. [CrossRef]
10. Parnaby, J. Concept of a manufacturing system. *Int. J. Prod. Res.* **1979**, *17*, 123–135. [CrossRef]
11. Shin, K.Y.; Shin, N.H.; Choi, S.W.; Choi, S.H. Systems engineering approach to designing smart condition monitoring systems for smart manufacturing (iccas 2016). In Proceedings of the 2016 16th International Conference on Control, Automation and Systems (ICCAS), Gyeongju, Korea, 16–19 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1177–1182.
12. Alhasnawi, B.N.; Jasim, B.H.; Sedhom, B.E.; Hossain, E.; Guerrero, J.M. A New Decentralized Control Strategy of Microgrids in the Internet of Energy Paradigm. *Energies* **2021**, *14*, 2183. [CrossRef]
13. Jost, J.; Kirks, T.; Mättig, B. Multi-agent systems for decentralized control and adaptive interaction between humans and machines for industrial environments. In Proceedings of the 2017 7th IEEE International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2–3 October 2017; pp. 95–100. [CrossRef]
14. Wang, P.; Govindarasu, M. Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid. *IEEE Trans. Smart Grid* **2020**, *11*, 3447–3456. [CrossRef]
15. PROFIBUS & PROFINET International. *PROFINET System Description Technology and Application*; PROFIBUS and PROFINET International: London, UK, 2012.
16. Raspberry Pi Foundation. *Raspberry Pi 4 Computer MODEL B*; Raspberry Pi Foundation: Cambridge, UK, 2019. Available online: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/ (accessed on 4 October 2021).
17. Khorrami, F.; Krishnamurthy, P.; Karri, R. Cybersecurity for Control Systems: A Process-Aware Perspective. *IEEE Des. Test* **2016**, *33*, 75–83. [CrossRef]
18. Dawson, M. Cyber security in industry 4.0: The pitfalls of having hyperconnected systems. *J. Strateg. Manag. Stud.* **2018**, *10*, 19–28.
19. Frank, A.G.; Dalenogare, L.S.; Ayala, N.F. Industry 4.0 technologies: Implementation patterns in manufacturing companies. *Int. J. Prod. Econ.* **2019**, *210*, 15–26. [CrossRef]
20. Working Group on Centralized Substation Protection and Control; IEEE Power System Relaying Committee. Advancements in Centralized Protection and Control Within a Substation. *IEEE Trans. Power Deliv.* **2016**, *31*, 1945–1952. [CrossRef]
21. Luejai, W. Automated Storage and Retrieval System using FIFO Method via PLC-integrated Human Machine Interface. In Proceedings of the 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 9–22 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1002–1005.
22. Brown, S. Functional safety of electrical machines and drives. In *1997 Eighth International Conference on Electrical Machines and Drives*; Conf. Publ. No. 444; IET: London, UK, 1997; pp. 326–330.
23. Giannoutsos, S.V.; Manias, S.N. A data-driven process controller for energy-efficient variable-speed pump operation in the central cooling water system of marine vessels. *IEEE Trans. Ind. Electron.* **2014**, *62*, 587–598. [CrossRef]
24. Skripcak, T.; Tanuska, P.; Konrad, U.; Schmeisser, N. Toward nonconventional human–machine interfaces for supervisory plant process monitoring. *IEEE Trans. Hum.-Mach. Syst.* **2013**, *43*, 437–450. [CrossRef]
25. Sinuraya, E.W.; Nugraheni, N.; Sukmadi, T.; Warsito, A.; Nugroho, A.; Soetrisno, Y.A.A. Design of Web Based Based Human Machine Interface (HMI) for Electric Tube Furnace. *Int. J. Comput. Eng. Inf. Technol.* **2018**, *10*, 201–207.
26. Jeng, S.L.; Chieng, W.H.; Chen, Y. Web-Based Human-Machine Interfaces of Industrial Controllers in Single-Page Applications. *Mob. Inf. Syst.* **2021**, *2021*, 6668843. [CrossRef]
27. Bakule, L. Decentralized control: An overview. *Annu. Rev. Control* **2008**, *32*, 87–98. [CrossRef]
28. Clark, R. Mobile HMI: Improves plant operations. *Control Eng.* **2016**, *63*, 30–33.

29. ICONICS, MobileHMI, 2017. Available online: https://www.iconics-uk.com/sites/default/files/productbrochure/MobileHMI_1.pdf (accessed on 4 October 2021).
30. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
31. Khan, W.Z.; Rehman, M.H.; Zangoti, H.M.; Afzal, M.K.; Armi, N.; Salah, K. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Comput. Electr. Eng.* **2020**, *81*, 106522. [CrossRef]
32. Beresford, D. Exploiting siemens SIMATIC S7 PLCS. *Black Hat USA* **2011**, *16*, 723–733.
33. Siemens. SIMATIC Controller-Take Control of the Future. 2021. Available online: https://new.siemens.com/global/en/products/automation/systems/industrial/plc.html (accessed on 4 October 2021).
34. Siemens. Remote Access to SIMATIC HMI Comfort Panels. 2020. Available online: https://cache.industry.siemens.com/dl/files/153/109476153/att_1016758/v3/109476153_Remote_Panels_HTML_V16_DOC_en.pdf (accessed on 4 October 2021).
35. Morris, T.H.; Gao, W. Industrial control system cyber attacks. In Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1, Leicester, UK, 16–17 September 2013; pp. 22–29.
36. Candell, R.; Stouffer, K.; Anand, D. A cybersecurity testbed for industrial control systems. In Proceedings of the 2014 Process Control and Safety Symposium, Houston, TX, USA, 6–9 October 2014; pp. 1–16.
37. Hogan, M.; Piccarreta, B.; Interagency International Cybersecurity Standardization Working Group. *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2018.
38. Sangodoyin, A.O.; Akinsolu, M.O.; Pillai, P.; Grout, V. Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning. *IEEE Access* **2021**, *9*, 122495–122508. [CrossRef]
39. Zhang, F.; Kodituwakku, H.A.D.E.; Hines, J.W.; Coble, J. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4362–4369. [CrossRef]
40. Gupta, U. Application of Multi factor authentication in Internet of Things domain. *arXiv* **2015**, arXiv:1506.03753.
41. Feng, X.; Babatunde, O.; Liu, E. Cyber security investigation for Raspberry Pi devices. *Int. Ref. J. Eng. Sci.* **2017**. Available online: https://uobrep.openrepository.com/handle/10547/622090 (accessed on 4 October 2021).
42. Electronics, S. Samsung Galaxy S2 Tablet: User Manual. 2016. Available online: https://www.samsung.com/uk/support/model/SM-T810NZKEBTU/#downloads (accessed on 4 October 2021).
43. Richardson, M.; Wallace, S. *Getting Started with Raspberry PI*; O'Reilly Media, Inc.: Newton, MA, USA, 2012.
44. Netgear Inc. Datsheet 300 Series-Plus Gigabit Ethernet Switches. 2021. Available online: https://www.netgear.com/images/datasheet/switches/GS305E_GS308E_DS.pdf (accessed on 4 October 2021).
45. Berger, H. *Automating with SIMATIC S7-1200: Configuring, Programming and Testing with STEP 7 Basic*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
46. Siemens. *SIMATIC S7-1200 Easy Book: Device Manual*; Siemens: Munich, Germany, 2015.
47. Fritz Studer AG. S33. 2019. Available online: https://cdn.studer.com/fileadmin/content_live_2019/www.studer.com/01_pdf/01_brochures/englisch/s33-brochure_studer_en.pdf (accessed on 4 October 2021).
48. FANUC CORPORATION. Fanuc Series Oi-Model F. 2014. Available online: https://www.fanuc.co.jp/en/product/cnc/fs_0i-fplus.html (accessed on 4 October 2021).
49. Raspberry Pi Foundation. *Datasheet: Raspberry Pi 4 MODEL B*; Raspberry Pi Foundation: Cambridge, UK, 2019.
50. Spring, J.; Nelson, D.; Lu, X.Y. *CACC Truck Instrumentation and Software Development*; Technical Report; Institute of Transportation Studies at UC Berkeley: Berkeley, CA, USA, 2018.
51. Wang, L.; Mahulea, C.; Júlvez, J.; Silva, M. Minimum-time control for structurally persistent continuous Petri Nets. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 2771–2776. [CrossRef]
52. Zhang, C.; Jiang, P. RFID-Driven Energy-Efficient Control Approach of CNC Machine Tools Using Deep Belief Networks. *IEEE Trans. Autom. Sci. Eng.* **2020**, *17*, 129–141. [CrossRef]
53. Liu, Y.; Xiahou, K.; Wang, L.; Wu, Q.H. Switching Control of GSC of DFIGWTs for Disturbance Rejection Based on Bang–Bang Control. *IEEE Trans. Power Deliv.* **2018**, *33*, 3256–3259. [CrossRef]
54. O'Brien, R. Bang-bang control for type-2 systems. In Proceedings of the 2006 Proceeding of the Thirty-Eighth Southeastern Symposium on System Theory, Cookeville, TN, USA, 5–7 March 2006; pp. 163–166. [CrossRef]