16th July 2023

ICAI Factory Digital Twin

Gonzalo Carrasco Velilla
Comillas Pontifical University, Madrid, Spain

Corresponding author: Gonzalo Carrasco Velilla (e-mail: gonzalo.carrasco97@gmail.com).

ABSTRACT This project covers the implementation of Namur's Open Architecture (NOA) in ICAI's factory to enable its digitalisation and integration into the connected era, preserving its original security and integrity. The solution involves the secure extraction of information from the factory equipment's and non-intrusive sensors, storing and consolidating all data in an OPC UA aggregate server. For its successful implementation, a NOA diode is designed with the necessary components to extract the data securely without compromising the factory's operations. These elements include OPC UA clients, Monitoring and Optimisation sensors, and an optocoupler-based data diode. The project incorporates an IoT gateway as the hardware platform to execute the solution, accompanied by the development of a SCADA dashboard to showcase a real-life application powered by NOA.

INDEX TERMS NOA, OPC UA, SCADA, IoT Gateway, Data Diode, M+O System

I. INTRODUCTION

The increasing demand for optimisation and the progress of digital transformation have created a pressing need to modernise the industrial sector. The conventional automation pyramid, backbone of industrial processes for centuries, has failed to adapt to new technological advancements like cyber-physical systems, digital twins, and AI-driven optimisation due to its inflexible and closed structure.

To tackle these challenges, new architectures are being developed to integrate Industry 4.0 technologies into industrial processes. Examples of these architectures include NOA (Namur Open Architecture) and O-PAS (Open-Process Automation Standard).

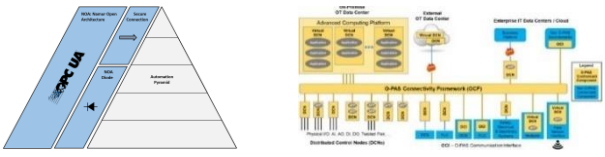

FIGURE 1. NOA vs O-PAS. NOA focuses on modernising industrial plants while integrating emerging technologies without disrupting production operations (Mondejar, 2023). On the other hand, O-PAS aims to establish an "open" model that interconnects all components within a factory.

These innovative architectures are made possible by OPC UA, a communication standard that has become essential in digitalisation projects and is projected to be the de-facto standard for exchanging information across the industrial sector, bridging the gap between OT and IT.

II. STATE OF THE ART

In recent years, NOA has emerged as a popular approach to enhance data interoperability across different layers in automation. It offers parallel integration, making it possible to develop digitalisation projects in brownfield plants that follow conventional architectures. However, as highlighted in a recent study by (Pontarolli, Bigheti, Sá, & Godoy, 2023), other solutions based on Microservice-Oriented Architectures (MOA), such as O-PAS, are emerging as viable and appealing options for green plants.

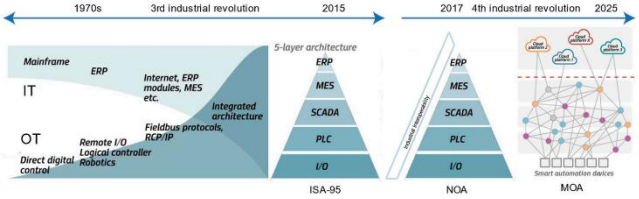

FIGURE 2. Timeline for IT-OT convergence (Pontarolli, Bigheti, Sá, & Godoy, 2023). To minimise disruption to ICAI's factory, a non-intrusive approach is essential. Thus, the adoption of NOA is the most effective solution as it preserves the existing automation pyramid, allowing for its implementation without disturbing the plant's day-to-day activities.

As emphasised earlier, the technological feasibility of these architectures relies on the adoption of an open and standardised communication interface, such as the OPC UA standard. The standard is developed and continuously improved by the OPC Foundation, an organisation comprised of industry leaders such as ABB, KUKA, Schneider Electric, and Siemens.

Numerous projects have emerged focusing on the development and design of OPC UA servers and clients, utilizing various frameworks and programming languages. The recommended method involves utilizing Microsoft's .NET framework, as the OPC Foundation offers its own SDK equipped with essential tools, libraries, and documentation. Although Python libraries are also available and are popular for their ease of use (González & BorgesRivero, 2022), their performance limitations often restrict their application to prototyping scenarios.

In addition to NOA and OPC UA, predictive maintenance has become increasingly valuable in proactively identifying, through sensor data collected in Monitoring and Optimisation Systems, the status and health of equipment (Zonta, et al., 2020). Employing cutting-edge technologies like machine learning, artificial intelligence, and data analytics, predictive maintenance can achieve cost reductions, minimised downtime, improved productivity, and enhanced product quality (Matyas, Nemeth, Kovacs, & Glawar, 2017).

Additionally, the use of digital twins in the industry has also been growing rapidly in recent years, with many companies acknowledging the benefits of having virtual replicas of their physical assets (Piromalis & Kantaros, 2022).

Finally, the topic of "cybersecurity in the new connected industry" is becoming ever more important. In the past, industrial systems were designed to operate in isolated environments, ensuring that production processes could run securely. However, with the integration of advanced technologies, such as IoT and Big Data analytics, the merging of industrial systems with enterprise networks has become more frequent, resulting in new security threats (Asghar, Hu, & Zeadally, 2019). Thus, to successfully mitigate these risks and safeguard critical infrastructure, the implementation of frameworks, such as NIST, has become crucial to proactively address vulnerabilities and ensure the integrity of entire industrial systems.

III. OBJECTIVES

1. Previous Studies: Study the available technologies for implementation and select the most suitable ones for the factory.

2. NOA Architecture and Information Model: Design the new architecture for the factory using the concepts provided by NOA, with OPC UA as the main building block. Develop a comprehensive information model that accurately represents the factory's elements and hierarchies, providing a clear understanding of its overall operations.

3. OPC UA Server and Clients: Develop the necessary OPC UA servers and clients to communicate and interconnect the system.

4. Monitoring and Optimisation sensors: Establish a system that will allow the massive installation of sensors to develop new projects related to predictive maintenance of industrial hardware. Configure the Siemens IOT2050 gateway to implement the M+O System and data diode.

5. SCADA Dashboard: Design a SCADA dashboard that can graphically represent all data from the factory's operations through the information model.

6. Cybersecurity Study and Secure Network Architecture: Conduct an in-depth cybersecurity study of the proposed solution.

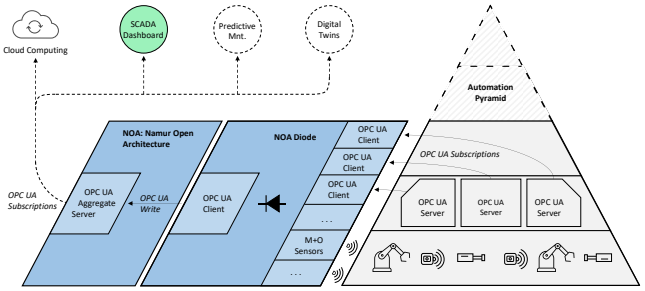

FIGURE 3. NOA implementation in ICAI's factory. The system consists of several essential components that facilitate secure data extraction from the factory while ensuring the reliability and robustness of the automation pyramid. At the core of the system is the aggregate server, developed using .NET and the OPC Foundation SDK. This server acts as a centralised hub, collecting and consolidating data from various sources within the manufacturing plant.

IV. TECHNOLOGY

To grasp and understand the execution of the project, an overview of the most important technologies is undertaken.

A. OPC CLASSIC

OPC Unified Architecture (OPC UA) is a standard developed by the OPC Foundation, building on the legacy of OPC Classic. The goal of this first standard was to standardise the information flow from the process level to the management level (MES, ERP, etc.), making it easier to integrate HMIs and SCADA systems and provide "real-time", "historical" and "event" data to management level applications.

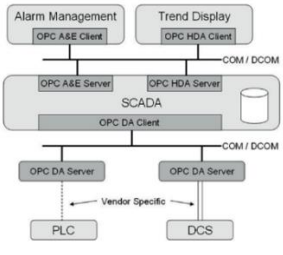

FIGURE 4. Typical example of clients and servers in Classic OPC (Mahnke, Leitner, & Damm, 2009). OPC Classic has three specifications: Data Access (DA), Alarm and Events (A&E), and Historical Data Access (HDA). The system uses a client-server approach, where servers store data from different sources of information, and clients connect to them to access and consume the data.

Classic OPC interfaces were originally constructed using COM (Component Object Model) and DCOM (Distributed COM) technologies from Windows, enabling the standard to have a rapid time-to-market. This initial approach was critical for the success of Classic OPC, but it also imposed important limitations on the standard.

Some of the main disadvantages in relation with its communication mechanism include:

- Limited cross-platform compatibility: OPC Classic relies on Windows platform protocols, which restrict its usage to Windows-based computers and servers.
- Compatibility issues with modern network environments: DCOM communications are not compatible with network environments containing Network Address Translation (NAT) or requiring communication through firewalls.
- Inability to facilitate Internet communication: The COM and DCOM communications employed in OPC Classic lack support for communication over the Internet. This limitation hinders the standard's adaptability to new IoT solutions and connected industry scenarios.

Additionally, OPC Classic suffers from limitations in its information modelling capabilities. This becomes apparent when analysing the data transmitted through OPC's DA, A&E, and HDA, as it is confined to basic pieces of information that lack comprehensive details regarding the overall condition of the factory.

For instance, when utilising OPC Classic, a temperature sensor reading is communicated without accompanying information about the sensor's type, precision, or engineering units (e.g., Celsius). Consequently, the transmitted information lacks the context needed to fully interconnect the organisation's infrastructure. This restriction primarily confines the standard's functionality to basic applications such as SCADAs and HMIs, limiting its potential for more advanced use cases.

B. OPC UA

In response to these challenges, the OPC Unified Architecture was developed to create a platform-independent standard that could replace all COM-based communications while maintaining the performance and features that made the original OPC successful. This new standard was designed to enhance the reliability of its transport mechanism, enable communication over the Internet, and incorporate crucial security and access control features.

Additionally, the new standard addressed the growing complexity of manufacturing systems through a significant improvement of its information models, achieving greater scalability, processing more intricate data, and enabling interoperability between manufacturers.

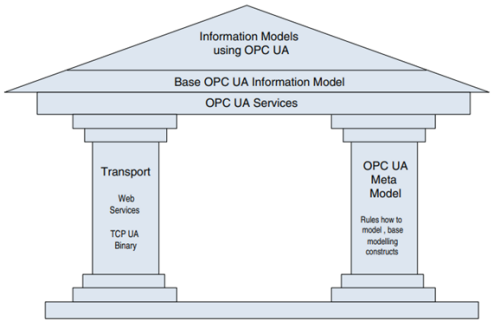

FIGURE 5. OPC UA Standard (Mahnke, Leitner, & Damm, 2009). The OPC UA standard comprises several layers that build upon two key components: the transport mechanism and the new data modelling.

Layer 1. OPC UA Services

The bottom layer comprises the OPC UA Services, which are responsible for establishing the service-oriented architecture within the standard. By doing so, OPC UA servers can provide services, such as "read", "write", or "subscribe", which clients can call to access data rapidly and effectively. This reduces the overall complexity of the data exchange process while improving its readability, reusability, and maintainability.

Layer 2. Base OPC Information models

As information models must be consumed by various applications, the new standard includes consistent rules around how they must be built and presented, ensuring that all systems using OPC UA can understand them. Thus, this layer defines the basic modelling blocks from which more complex models can be constructed, ensuring consistency between different applications.

Layer 3. Information models using OPC UA

The third layer encompasses specific information models built on the OPC UA framework. These models define the structured format of data exchanged between servers and clients and they offer the flexibility to be customised and tailored to meet specific use cases and requirements.

Transportation mechanisms

The transport mechanism plays a critical role in OPC UA by defining the protocols that establish connections between all elements within the framework. It ensures secure and reliable communication, facilitating data exchange, and promoting interoperability across servers and clients.

The OPC UA standard introduces various transport mechanisms for data transfer:

- Web Services using SOAP and HTTP: is well-suited for scenarios where firewalls are present, allowing data transfer without requiring complex configuration changes or network setups.
- Optimised binary TCP: designed to facilitate high-performance, low-latency and real-time communications.

These platform-independent protocols enable OPC UA to operate on a vast range of hardware, software platforms and operating systems, making it incredibly adaptable and compatible with various industrial settings. This flexibility allows OPC UA to run on low-performance IoT devices, high-end servers, PLCs, DCS or SCADAS, while being easily integrated with enterprise-level software such as MES and ERP systems.

Data modelling

With regards to the data modelling component, OPC UA adopts an object-oriented approach to create complex information models, enabling the accurate representation of intricate systems and hierarchies. This foundation becomes particularly valuable in the context of conventional industrial environments that rely on the automation pyramid.

In these environments, communication is typically limited to adjacent layers due to the isolation imposed by distinct communication networks. However, the advent of IIoT standards like OPC UA has revolutionised the communication landscape, eliminating these network boundaries and fostering a decentralised communication system that transcends traditional layer-based constraints.

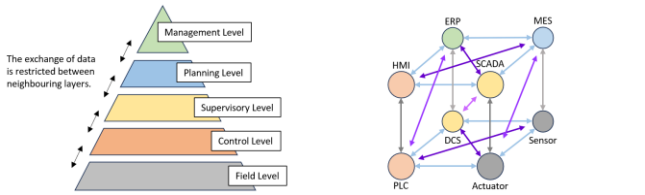

FIGURE 6. Traditional vs Decentralised communications (Represa, et al., 2023). To achieve effective communication in decentralised systems, it is crucial to ensure consistency of data in terms of its information representation. This entails representing information in a uniform manner across all five levels.

Thus, the objective of information models is to provide every element in the factory's environment with a full view of all other components, understanding not only the basic data (temperature in case of a field-level sensor) but also its context and situation within the factory (Industry40tv, 2020b).

C. M+O SENSORS

The project's Monitoring and Optimisation sensor system, designed to extract valuable insights from the factory floor, focuses on the utilisation of Modbus sensors.

Modbus RS-485 is a serial communication protocol commonly employed in industrial automation and control systems. The protocol operates on a master-slave architecture, where the master device, such as a PLC or IoT gateway, initiates communication by sending requests to the connected slave devices, such as sensors and actuators.

RS-485 is designed for half-duplex and multipoint communications, enabling the connection of up to 247 slave devices on the same bus. The master device supports two modes of communication:

- Unicast mode: where the master communicates with a single slave device by directing the message to its unique address.
- Multicast mode: used to broadcast a message to all slave devices without expecting any response from them. Consequently, only "write" messages can be sent.

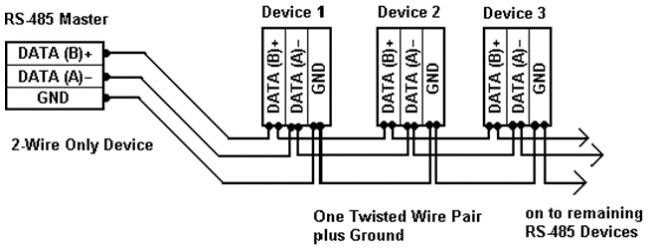

FIGURE 7. Modbus RS-485 Physical Layer. Communication in Modbus RS-485 occurs via a twisted pair of wires utilising differential signalling. This means that data is transmitted as voltage differences between two data lines, typically referred to as Line A and Line B, enhancing noise immunity and enabling long-distance transmission.

D. DATA DIODE

To ensure robust security measures, a data diode based on RS-232 communication is implemented, establishing a connection between the IoT gateway and the external devices. This data diode serves as a unidirectional channel, enabling controlled data transmission solely from the IoT gateway to external systems while preventing any inbound communication.

RS-232 is a widely adopted protocol for serial communication, commonly employed in computer systems and industrial applications. Unlike RS-485, which utilises differential signalling, RS-232 employs a single-ended signalling method, where voltage levels are measured to a common ground.

Data is transmitted sequentially, one bit at a time, over a single data line, allowing communication between two devices: a transmitter and a receiver. Additionally, it operates in full-duplex mode, enabling simultaneous bidirectional communication.

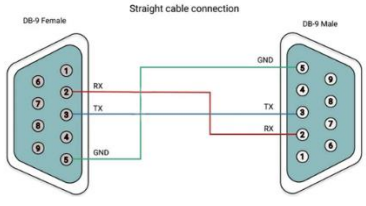

FIGURE 8. RS-232 Physical Layer (Anticyclone Systems, 2023). DB-9 connectors are utilised to establish the physical connection, employing specific pin assignments for data transmission (Tx), data reception (Rx), and ground (GND) signals.

V. IMPLEMENTATION AND DEPLOYMENT

This chapter provides an in-depth overview of the work conducted throughout the project.

The implementation phase begins with the development and integration of the information model into the OPC UA aggregate server, establishing a common interface for data exchange among the system's elements. Then, the section covers the creation of the NOA diode with its OPC UA clients, Monitoring and Optimisation sensors, and an optocoupler as its communication channel. The main goal of these elements is to connect the factory's equipment and non-intrusive sensors with the newly created server.

Additional attention is given to the configuration and installation of the hardware devices, specifically Siemen's IOT2050 gateway. Finally, the chapter outlines the development of the SCADA dashboard, showcasing a real-life application empowered by NOA.

A. INFORMATION MODEL

The primary goal of the information model is to depict the structure, behaviour, and semantics of the data within the factory, allowing client-server communication between devices running OPC UA applications.

Base device type

To ensure precise representation of objects and their essential attributes, the factory's information model incorporates a "base device" ObjectType.

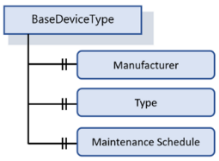

FIGURE 9. BaseDeviceType. Serves as a standardised template for all Object and ObjectType nodes that will be subsequently defined. The "Manufacturer", "Type", and "Maintenance schedule" attributes are important and common to all devices in the factory as they provide information for efficient operation, maintenance, and planning.

Basic sensors and actuator types:

Having established the foundational device base type, the next phase entails the definition of Node ObjectTypes for the factory's sensors and actuators.

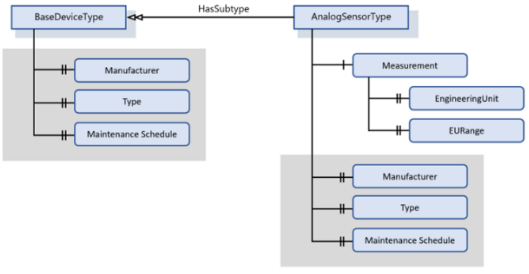

FIGURE 10. Basic analog sensor schema. In addition to analog sensors, actuators and digital sensors are also modelled.

Specific sensors and actuators

Afterwards, the information model includes more specific devices such as analog temperature and humidity sensors, digital proximity sensors, and various types of actuators like pneumatic pistons, conveyors, and robots.

Integrated Modules

Once the foundational elements of the factory are defined, the subsequent step involves creating the more complex modules that comprise it.

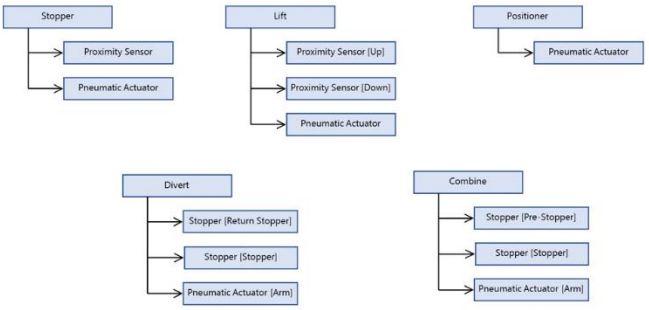

FIGURE 11. Integrated modules. Drawing upon the details provided about the factory's blueprints and components, the schemas for stoppers, lifts, positioners, diverts, and combines are formulated.

Stations

The modules are then integrated into the information model of the factory workstations, representing the physical workstations and their associated devices.

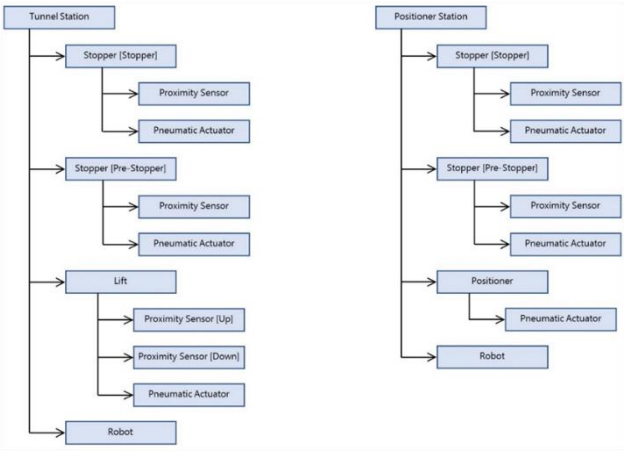

FIGURE 12. Stations. In the factory there are two types of stations: "Tunnel Stations", equipped with lifts that raise the pallets to the workspace where the robots perform their operations. And "Positioner Stations", which have their own conveyor belts and are equipped with positioners that lock pallets in place. Each station is also fitted with two stoppers or retainers, that allow operators to control the flow of material within each station.

Factory

To complete the information model, the modules and stations are consolidated within a single folder-type object node called "Factory." The Factory node is organised into two primary sectors: Stations and Conveyors. The Conveyors sector further subdivides into Conveyor Belts

and Conveyor System Controls, providing a clear separation between the physical belts and the actuators responsible for guiding the pallets throughout the factory.

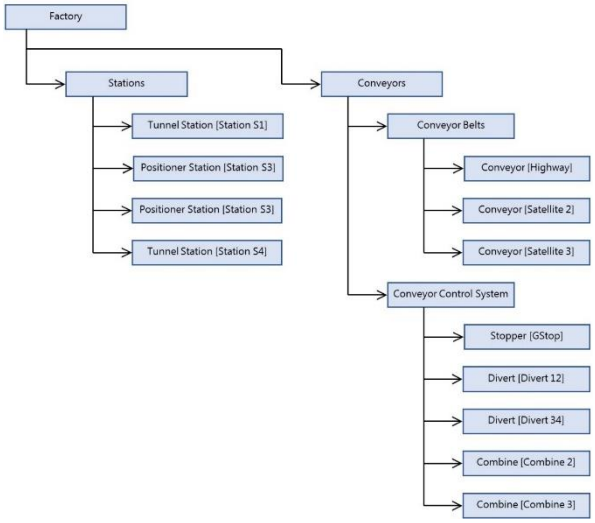

FIGURE 13. ICAI factory. It is a compact production facility consisting of four interconnected stations. The main conveyor belt, known as the "highway," forms the backbone of the entire production process, facilitating the movement of pallets between stations. Additionally, the factory uses control mechanisms, known as diverts and combines, that are installed in the main conveyor belt to control pallet flow.

B. OPC UA AGGREGATE SERVER

Communications in OPC UA operate on a client-server model. Servers are responsible for storing data from various sources, while clients utilise services provided by the servers, such as read, write, or subscribe to monitor, control, and visualise the data.

The current section focuses on the development of an aggregate server that acts as a centralised repository for all data generated within the factory. Regarding the sources of information, the project relies on OPC UA servers deployed on each of the factory's S7-1500 PLCs and the readings from M+O sensors.

The server is built using the .NET framework and the OPC Foundation's SDK. To accomplish this, the XML file that contains the factory's information model is compiled, arranging the data in a hierarchical structure that is intuitive and easy to understand.

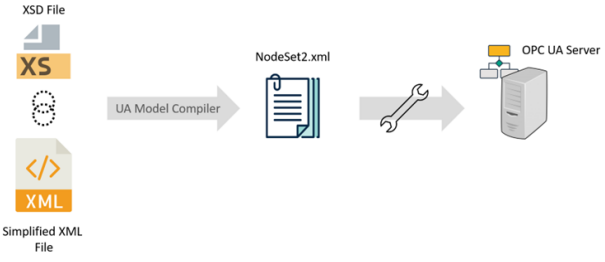

FIGURE 14. OPC UA Server Build Process Diagram (Original work). The UAModelCompiler is an essential component of the OPC Foundation's toolkit, as it guarantees adherence to OPC UA standards while simplifying the generation of files needed for the server's construction.

Bellow, a screenshot of the server application is provided, offering a visual representation of its user interface. Additionally, an extensive list of integrated features within the server application is presented, highlighting the wide range of features it offers.

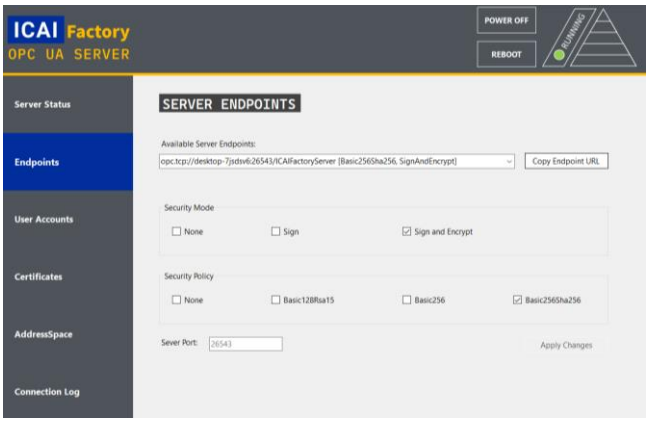

FIGURE 15. Aggregate server desktop application.

Firstly, to browse the server application, a side panel is provided to navigate through its various menus:

- Server Status: This menu presents the current server status (running, stopped, etc.), along with the server's start time and the URL required to establish a connection.
- Endpoints: Within this section, users can access a list with all available endpoints for the server and configure the security policies and modes.
- User Accounts: This menu serves as a platform for managing authentication mechanisms. Administrators can create, view, and delete user accounts, as well as configure the specific type of authentication required for accessing the server through a client (Anonymous, Username and Password, X509 Certificate).
- Certificates: Both untrusted and trusted certificates are displayed, providing administrators with the capability to effectively manage certificate distribution. This includes controlling which clients are granted trust for establishing connections. Moreover, the app enables the deletion of rejected certificates and provides the option to accept untrusted certificates if deemed necessary.
- AddressSpace: Represented as a simple tree structure, this menu grants users access to a comprehensive display of all object nodes within the address space. It facilitates a clear understanding of the server's information model.
- Connection Log: The connection log menu empowers users to monitor and track login attempts. This log provides detailed information on successful connections to the server and authentication failures, serving as a valuable security tool and allowing users to export the log data as a plain text file.

Finally, two buttons located at the top right corner allow users to turn the server ON or OFF and initiate a reboot. This functionality is noteworthy because configuration changes require restarting the server for them to take effect.

C. NOA DIODE

The NOA diode incorporates all the essential components needed to transfer data, from the factory to the aggregate server, through a secure and unidirectional connection.

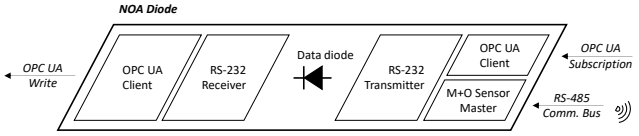

FIGURE 16. NOA diode (Original work). It consists of two OPC UA clients, a master program for the RS-485 bus, and the necessary RS-232 transmitter and receiver. Physically, the NOA diode is built using the IOT2050, hosting the components to the right of the diode, a 4N35 optocoupler (as the data diode itself), and by one lab computer that runs the receiver and client to the left of the diode.

OPC UA Clients

One of the primary elements of the NOA diode are the OPC UA clients, responsible for connecting with the factory's equipment and subsequently transmitting the information to the aggregate server. Node-RED is employed to develop these clients, using the dedicated OPC UA library "node-red-contrib-opcua".

1. The first client application is responsible for extracting data from the factory's PLCs and transmitting it through the data diode using the RS-232 communication protocol.

2. The second client application receives RS-232 messages and writes them into the aggregate server.

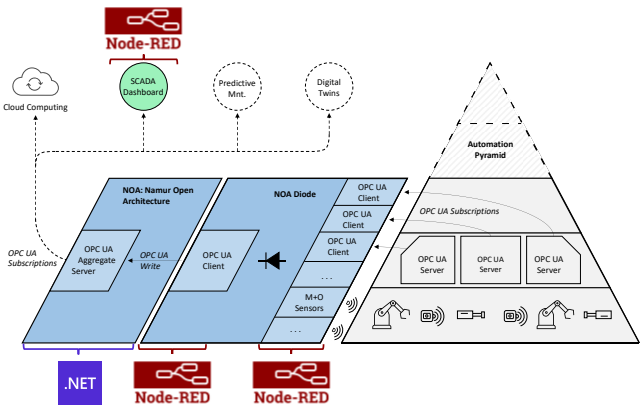

FIGURE 17. Software development tools and environments used to build OPC UA Servers and Clients (Original work). NOTE: to extract and transfer data from the factory's PLCs to the aggregate server, it is necessary to develop a dedicated OPC UA client for each OPC UA server running on a PLC.

M+O Sensors

The Monitoring and Optimisation sensors play a crucial role in facilitating future predictive maintenance projects and optimisation initiatives within the factory. Their primary objective is to extract valuable information from field devices and provide it to predictive maintenance applications. This proactive approach ensures operational efficiency, minimizes downtime, and maintains the smooth operation of critical equipment. Through the capture of relevant data, these sensors significantly contribute to maximizing productivity and prolonging the lifespan of machinery and systems.

To align with the principles of NOA, it is essential that the new sensors from the M+O System are non-intrusive, meaning they do not interfere with the factory's existing automation pyramid. Consequently, the control mechanism for these sensors must not rely on the factory's PLCs responsible for running the processes. Instead, an external device capable of independent monitoring is employed. In this case, the IOT2050 gateway serves as the control system for the non-intrusive sensors.

The current project includes basic temperature and humidity Modbus sensors, but it also has the capability to incorporate modern protocols like MQTT and other wireless connectivity mechanisms. To control the M+O sensors, the IOT2050 assumes the role of a Modbus master, periodically polling the sensors to retrieve the measured data.

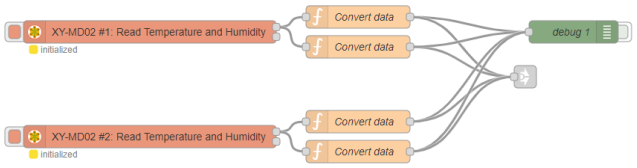

FIGURE 18. Modbus master project. The "node-red-contrib-modbus" library is used to incorporate the necessary nodes.

Data Diode

Designing and constructing the physical data diode is central to implement NOA's architecture, as it safeguards the automation pyramid and prevents external access to the field devices.

To mitigate the high costs associated with UDP based commercial data diodes, an alternative and more cost-effective solution is implemented using RS-232.

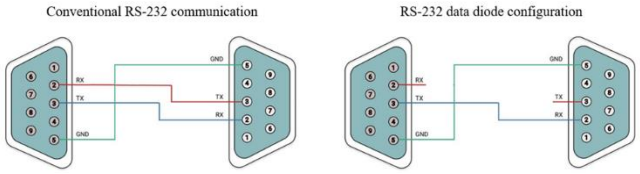

FIGURE 19. RS-232 conventional vs data diode communication (Original work). To construct a basic data diode, it is sufficient to connect both ground signals and the Tx and Rx terminals of the respective transmitting and receiving devices. By only utilising these two wires, the data diode ensures unidirectional communication, allowing data to flow from the transmitting device to the receiving device while preventing any feedback or communication in the opposite direction.

While the configuration shown in Figure 19 prevents data transmission from the receiver to the transmitter, it is important to emphasise that robust cybersecurity data diodes typically necessitate a physical separation between the two devices. In this project, this is achieved through a 4N35 optocoupler.

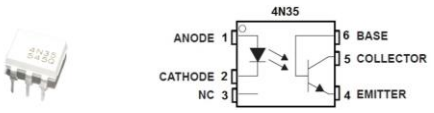

FIGURE 20. 4N35 Optocoupler. The physical separation inside the optocoupler ensures that bidirectional data transmission is impossible, regardless of the circumstances.

Design

Building upon this concept, a dedicated circuit has been meticulously designed to incorporate the optocoupler as the central component of the NOA diode. Rather than utilising a DB9 connector, the circuit employs a USB to RS-232 converter to interface with the communication line.

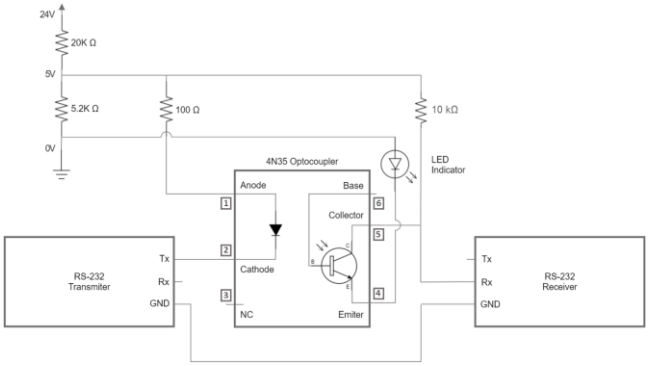

FIGURE 21. Data diode circuit diagram (Original work). To comprehend this specific configuration, it is crucial to recognise that the RS-232 converter utilises a particular voltage encoding scheme. In this scheme, a "0" bit is represented by a voltage level of +5 V, while a "1" bit is represented by a voltage level of 0V.

Prototyping and Product Assembly

After completing the circuit design, the subsequent step involves prototyping, to evaluate the circuit's functionality, and building the first MVP.

FIGURE 22. Data diode. The data diode is assembled using a PCB (Printed Circuit Board) and a specially adapted plastic case designed to be mounted on DIN rails. This feature is particularly significant as it enables the data diode to be conveniently installed alongside the IoT gateway.

Data Diode Limitations

The utilisation of RS-232 communication entails a notable limitation in terms of data bandwidth due to the constraints imposed by the serial protocol. Consequently, a series of tests are conducted to ensure that the current configuration can effectively handle the data from the PLCs and non-intrusive sensors.

Furthermore, due to the unidirectional nature of the communication, there is no confirmation of whether messages have been received correctly. This means that any messages containing bit errors will not be detected or notified to the transmitting device, resulting in potential data loss.

Another limitation to consider is data confidentiality and the risk of false messaging. Since RS-232 communications are sent without encryption, messages can be easily intercepted by connecting a device to the communication lines, compromising data confidentiality. Moreover, an attacker could exploit the data diode to send false information, interfering with the data sent to the server and undermining its validity.

D. HARDWARE. IOT GATEWAY

To successfully deploy the solution in the factory, the hardware devices must be carefully considered.

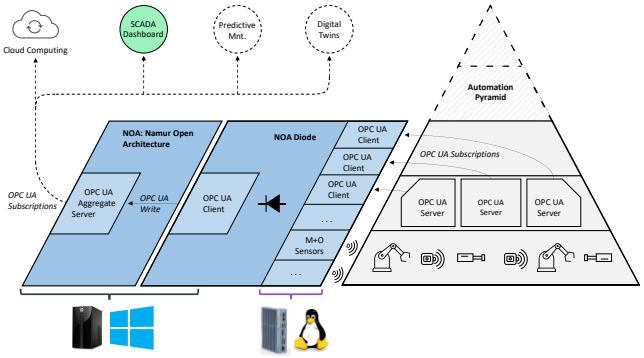

FIGURE 23. Hardware diagram. The IOT2050 gateway from Siemens has been specifically chosen for its suitability in industrial and IoT scenarios. It establishes the physical connection between the Windows machine, hosting the aggregate server, the PLCs, and the M+O System. Additionally, the gateway is equipped with various communication interfaces to enhance connectivity across its supported protocols. These interfaces comprise a serial communication port (COM), a DP port, two USB ports, and two Ethernet ports.

Through an SSH connection, the IOT2050 device can be remotely configured and managed. This allows users to configure network settings, install software packages, and monitor system performance, among many other things. By typing the command `iot2050setup`, a setup page is launched displaying all available configuration options for the IOT2050 device. These options encompass changing usernames and passwords, modifying its static IP address, managing software packages, and configuring peripherals.

Additionally, to ensure both safety and functionality, the IOT gateway is securely placed inside an electrical case mounted on a DIN rail. This enclosure protects the equipment and safeguards users from potential hazards such as electrocution or severe burns caused by the high temperatures of the gateway's heat sink.

One notable advantage of the setup is that the IOT2050 and the power supply are installed together in a single box. This consolidation of equipment offers the convenience of easy transportation and provides a compact and organised solution.

FIGURE 24. Gateway setup. The box includes power supply connectors that mitigate the risk of electrocution, along with Ethernet ports that allow direct connectivity to the case. This eliminates the need for threading RJ-45 connectors into the gateway ports, ensuring a simplified and efficient setup. Additionally, flexible USB connectors are incorporated to facilitate easy access to the ports of the device.

E. SCADA DASHBOARD

After successfully setting up all the software and hardware components, the subsequent task is to develop a Supervisory Control and Data Acquisition (SCADA) dashboard. This interface is built as a proof of concept to showcase NOA's potential, allowing operators to access and monitor all relevant information related to the factory operations. Through the SCADA dashboard, operators can visualise and analyse data in a detailed manner, providing them with valuable insights for effective decision-making.

Once again, Node-RED is used to develop this dashboard, utilising two specific libraries:

1. node-red-dashboard: enables the creation of dashboards with customisable widgets that can display data in various formats, including charts, tables, and gauges.
2. node-red-contrib-ui-svg: used to display an SVG image of the factory's operating elements, along with animations that reveal their status in the factory.

Factory Layout Display

Utilising the SVG library in Node-RED, a layout display for the factory floor is created based on its blueprints. This layout aims to accurately depict the physical arrangement of the factory and its associated hardware.

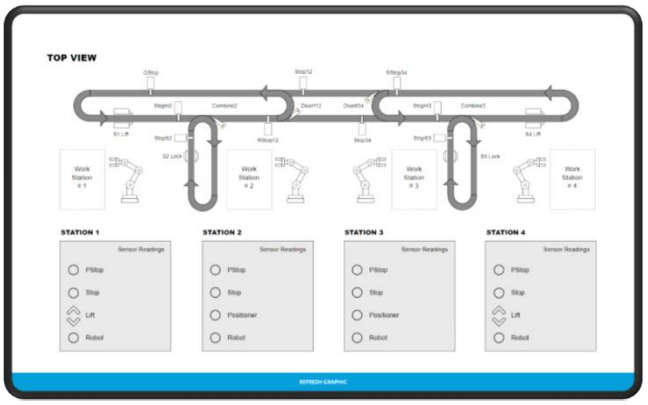

FIGURE 25. Factory layout display. To enhance visual representation, animations are incorporated into the layout to showcase the movement of pneumatic actuators and the conveyor control system, specifically the divert and combine needles.

Control Panels

In addition to the layout display, control panels are designed to provide a summarised and simplified representation of the data. These control panels are organised based on the various subsystems present in the factory, allowing operators to easily filter and access the relevant information as needed.

These panels include:

- Stations: offers details about the sensors, actuators, and robots present in each station. It allows operators to monitor the status and performance of these components, ensuring smooth operations and identifying any potential issues that may arise.
- Conveyor Belts: provides real-time updates on the status and speed of the three main conveyor belts: the highway, satellite 2, and satellite 3.
- Diverts and Combines: exhibits information about the needles within the conveyor control systems. It also includes details about the stoppers that prevent pallets from colliding with each other.
- Asset Management: provides information about the assets present in the factory. It includes details such as the manufacturer, payload capacity, maximum speed, asset type, and maintenance schedule.
- M+O sensors: employs gauges and a graph to represent temperature and humidity readings from the XY-MD02 sensors installed within the factory.

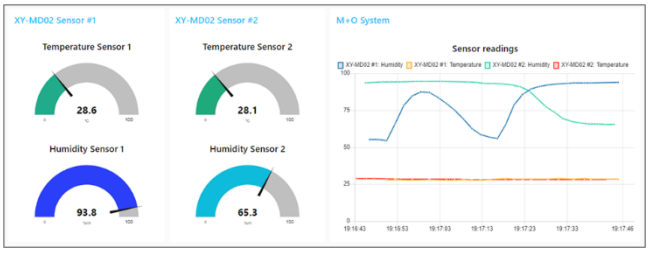

FIGURE 26. M+O System panel. Operators can monitor environmental factors in real-time, allowing for proactive measures to maintain optimal conditions within the facility.

VI. CYBERSECURITY STUDY

Finally, the project concludes with an in-depth cybersecurity study aimed at safeguarding the factory from malicious attacks. To comprehend the necessity of these studies, it is imperative to analyse the economic consequences that an attack could inflict upon the University and the factory. Therefore, a simplified cost analysis is conducted to assess the financial implications associated with such attacks.

Firstly, with focus on the factory, an attack could lead to a complete halt in operations, resulting in a significant economic impact. Assuming the factory produces goods valued at 25€ per unit and has a production capacity of 15 units per hour, a one-hour factory shutdown would result in a loss of 375 €. Extrapolating this to a week of work, accounting for 8 hours per day, the economic losses would amount to 15,000 €.

Additionally, the University's academic activities would also suffer the consequences of an attack. Considering that a class of students, consisting of 20-30 individuals, pays an average of 376 € per hour for lab usage, and assuming the lab is utilised for approximately 7.2 hours per day, the weekly costs would reach 13,536 €.

OPSEC analysis

The first guideline used for the security analysis consists of the OPSEC (Operations Security) framework, which is designed to identify and safeguard critical information through a methodical examination of potential threats and vulnerabilities.

The OPSEC framework consists of five phases: identifying critical information, analysing threats, discovering vulnerabilities, assessing risks, and developing countermeasures.

NIST analysis

The second framework used to conduct the cybersecurity study is the NIST framework, which provides comprehensive guidelines, standards, and best practices for cybersecurity risk management. It follows a five-step approach—identify, protect, detect, respond, and recover—helping evaluate vulnerabilities, detect anomalies, respond to incidents, and recover from disruptions.

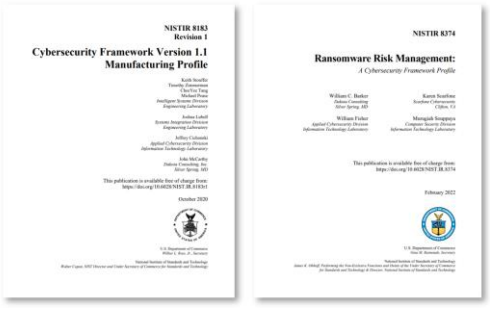

FIGURE 27. NIST guidelines used for the study. Within the NIST framework, two notable guidelines are utilised. Firstly, the "Manufacturing Profile" of the Cybersecurity Framework, which serves as a roadmap to help manufacturers reduce cybersecurity risks in accordance with industry best practices and sector-specific goals. Additionally, the analysis incorporates the "Ransomware Profile", which focuses on identifying, protecting, detecting, responding, and recovering from ransomware events.

Network Topology Design

After completing both studies and obtaining a comprehensive understanding of the vulnerabilities faced by the factory, this section covers the development of a secure architecture that could be implemented in the near future.

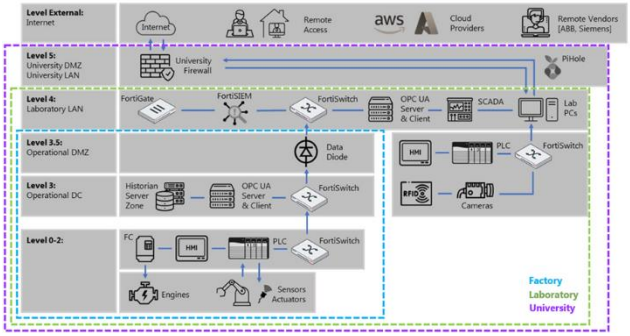

FIGURE 28. Secure architecture for ICAI's University and factory (Original work). The schematic diagram illustrates the division of the entire infrastructure into three distinct zones: the factory, the laboratory, and the University. This division serves to clearly delineate the roles of each element and the staff responsible for their future installation and maintenance.

VII. RESULTS

A. RESULTS

The main objective of this research project was to validate the implementation of NOA's architecture in ICAI's factory. Over a three-day period, rigorous testing and fine-tuning were conducted to achieve optimal performance, allowing to conduct a clear evaluation of the architecture's applicability in a real working environment.

During the testing phase, significant milestones were successfully achieved:

- The integration of the IOT gateway with the factory's PLCs was successfully accomplished, establishing a secure OPC UA connection through the laboratory network.
- Testing confirmed the correct execution of the master program running on the IOT2050 device. The RS-485 bus, featuring non-intrusive sensors, was successfully implemented to capture the intended temperature and humidity data.
- Secure transmission of data through the diode was accomplished, facilitating the transfer of information from the factory to the dedicated Windows machine.
- The Windows machine, responsible for hosting the aggregate server and SCADA dashboard, performed well during testing, ensuring real-time updates on the SCADA interface.

FIGURE 29. Project's results and overall summary.

Consequently, it can be concluded that the project's overall results have been highly satisfactory, as NOA was successfully implemented to fulfil the specific requirements of the factory and securely extract data for future digitalisation projects. This successful proof of concept demonstrates that NOA is not merely a theoretical concept, but a practical, compatible, and viable solution that can be seamlessly integrated into real-world scenarios and industrial settings.

B. DISCUSSION AND ANALYSIS

After assessing the overall results, this section highlights any limitations or challenges encountered during the project.

During the project's commissioning, limitations related to the server were identified. Problems arose when trying to connect to the OPC UA aggregate server from other machines in the same network. Currently, connecting to the server from a different computer requires conducting an SSH tunnel and port forwarding. While this limitation can be seen as a positive security measure, as it restricts access to the server, it also limits the system's usability.

Additionally, the use of a data diode for secure communication introduced challenges in the exchange of data. A prominent example of such challenges arises when the aggregate server necessitates an update of all variables. In this scenario, the sequencing of instructions cannot be directly ordered by either the dashboard or the server. Thus, an operator must undertake this task by accessing the IoT gateway positioned prior to the data diode.

Furthermore, the limited bandwidth of the RS-232 communications poses a scalability constraint. As the factory and M+O sensors will progressively grow, the increased data volume may surpass the capacity of the data diode to handle it effectively. This limitation could hinder the system's ability to accommodate future expansion and the integration of additional sensors. Therefore, it is crucial to consider this issue and assess the need for upgrading the data diode to a commercial-grade solution that can handle higher volumes of data.

VIII. CONCLUSIONS

While there is room for improvement in certain areas, the project has successfully achieved its main objective of deploying the NOA architecture in ICAI's factory. This deployment has facilitated the digitalisation and integration of the factory into the connected era while ensuring the preservation of its security and original integrity. Through the implementation of Namur Open Architecture, the project has enhanced operational capabilities, improved efficiency, and enabled real-time data-driven decision-making.

These accomplishments have set the bases for future digital transformation and optimisation, positioning the factory for upcoming advancements in areas such as predictive maintenance, big data analysis, and cloud computing. Thus, the project's success underscores the commitment to modernise the factory and embrace the opportunities of Industry 4.0, ultimately driving innovation and competitiveness in its operations.

IX. FUTURE WORK

Based on these notable achievements, ICAI factory showcases several promising areas for future advancements and developments.

One such area is the implementation of digital twins, which can be used to simulate and monitor the performance of machines and processes in real-time, enabling proactive maintenance and optimisation.

Predictive maintenance is another area that holds great potential. Through advanced analytics and machine learning algorithms, predictive maintenance can anticipate equipment failures and schedule maintenance activities accordingly.

In the field of big data, ICAI can take advantage of the vast volume of data generated by diverse systems and sensors within the factory, enabling the acquisition of valuable insights and facilitating data-driven decision-making. Making use of ICAI's cluster, numerous projects can be developed to further explore and analyse this data.

Furthermore, the secure connection to the internet unlocked by the NOA architecture enables the utilisation of cloud computing resources, such as scalable storage, computational power, and advanced analytics.

APPENDIX A
ALIGNMENT WITH SDGS

The digitalisation of industrial processes, including the implementation of the NOA architecture in ICAI's factory, aligns with the following Sustainable Development Goals (SDGs):

SDG 3: Good Health and Well-being

In manufacturing processes, many manual tasks are necessary to maintain plant operation, such as maintenance work. These duties, often known as "4D jobs", are characterised by being Dull (manual collection of parameters), Dirty, Dangerous, and Distant (they require workers to travel to remote locations where the factories are located). Thus, digitalisation seeks to eliminate these "4D" jobs and replace them with safer, less monotonous work that can be done remotely (Berge, 2022c).

SDG 8: Decent Work and Economic Growth

Digitalisation of industrial processes can lead to the creation of new jobs and better working conditions, particularly as it relates to eliminating dangerous, tedious, and monotonous tasks. This can contribute to economic growth and the promotion of decent work.

SDG 9: Industry, Innovation, and Infrastructure

The digitalisation of industrial processes enables innovation and the development of new technologies, that can improve efficiency, reduce emissions, and make manufacturing more sustainable. In this project, Namur Open Architecture helps streamline operations and facilitate the development of new "smart" applications such as predictive maintenance or the development of digital twins.

SDG 12: Responsible Consumption and Production

Digitalisation can help reduce waste and improve resource efficiency in manufacturing, making production more responsible and sustainable. By automating tasks and optimising processes, it's possible to reduce energy consumption and minimise its environmental impact.

SDG 13: Climate Action

Finally, digitalisation projects can play a critical role reducing emissions and mitigating climate change. By enabling a more precise monitoring of emissions, regulatory entities can measure all emissions produced by factories and industrial facilities in real time, forcing companies to comply with environmental regulations. Therefore, digital transformation does not only reduce emissions, but also provides the tools necessary, such as IIoT, to legislate them.

By aligning with these SDGs, the implementation of the NOA architecture in ICAI not only improves efficiency, energy consumption, and safety, but it also contributes to broader sustainability goals. Thus, this project will help to ease maintenance work, improve the academic lectures given at University, and create a platform for the development of new applications, promoting further innovation.

REFERENCES

Asghar, M. R., Hu, Q., & Zeadally, S. (2019, october 8). *Cybersecurity in industrial control systems: Issues, technologies, and challenges.* Retrieved from Google Scholar: https://www.sciencedirect.com/science/article/pii/S1389128619306292

Berge, J. (2017a, july 23). *Digital Transformation - What it Actually Means for a Plant.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/digital-transformation-what-actually-means-plant-jonas-berge

Berge, J. (2017b, december 19). *Starting Digital Transformation - Threat and Opportunity of the New Industrial Revolution.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/starting-digital-transformation-threat-opportunity-new-jonas-berge

Berge, J. (2018a, september 11). *Virtual Reality for Accelerated Field Operator Learning and More.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/virtual-reality-accelerated-field-operator-learning-more-jonas-berge

Berge, J. (2018b, october 21). *Standards for Automation - No Regrets Digital Transformation.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/standards-automation-regrets-digital-transformation-jonas-berge

Berge, J. (2019a, november 20). *Implementing the NAMUR Open Architecture (NOA).* Retrieved from LinkedIn: https://www.linkedin.com/pulse/implementing-namur-open-architecture-noa-jonas-berge

Berge, J. (2019b, november 27). *If it won't break, don't sense it.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/wont-break-dont-sense-jonas-berge

Berge, J. (2020a, march 10). *Enterprise OT - Structured Integration for Digital Transformation.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/enterprise-ot-structured-integration-digital-jonas-berge

Berge, J. (2021a, march 4). *Steer Your DX Project Through the Gate Process.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/steer-your-dx-project-through-gate-process-jonas-berge

Berge, J. (2021b, october 14). *7 Standards for HyperAutomation.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/7-standards-hyperautomation-jonas-berge

Berge, J. (2021c, december 27). *#BigIdeas2022 - Survive & Thrive HyperAutomation.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/bigideas2022-survive-thrive-hyperautomation-jonas-berge

Berge, J. (2022a, march 10). *Architecture: Flat or Structured ISA 95/Purdue.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/architecture-flat-structured-isa-95purdue-jonas-berge

Berge, J. (2022c, september 20). *M+O Sensors: Monitoring & Optimization.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/mo-sensors-monitoring-optimization-jonas-berge

Berge, J. (2022d, october 10). *The Technology Freedom Paradox.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/technology-freedom-paradox-jonas-berge

Csanyi, E. (2016, december 7). *9 Rules for correct cabling of the Modbus RS485 communication systems*. Retrieved from Eectrical Eineering Portal: https://electrical-engineering-portal.com/correct-cabling-modbus-rs485

González, I. J., & BorgesRivero, R. A. (2022). *Free software HMI application developed on Python to monitoring a hydraulic subsystem at the pediatric hospital La Balear of Havana.* Retrieved from RENIA: https://renia.cujae.edu.cu/index.php/renia/article/view/38

Industry40tv. (2020a, september 2). *What is OPC UA and How it Works?* Retrieved from YouTube: https://www.youtube.com/watch?v=vRk42W_4R0o&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7

Industry40tv. (2020b, september 15). *OPC UA Information Model - How an OPC UA Information Model Works*. Retrieved from YouTube: https://www.youtube.com/watch?v=f5oPEVhZFug&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=2

Industry40tv. (2020c, october 19). *Understanding OPC UA Base Information Model and Companion Specifications*. Retrieved from YouTube: https://www.youtube.com/watch?v=cL5Tq7a1gwo&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=3

Industry40tv. (2021a, enero 19). *OPC UA .NET Tutorial - Creating Information Model and OPC UA Server Using NET*. Retrieved from YouTube: https://www.youtube.com/watch?v=gxA7SDNLHgc&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=4

Industry40tv. (2021b, june 10). *How OPC UA Client Server Communication Works*. Retrieved from YouTube: https://www.youtube.com/watch?v=vgE9P6KNC7g&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=5

Industry40tv. (2021c, october 13). *OPC UA Technology Mapping: Data Encoding, Data Security and Transport Protocols*. Retrieved from YouTube: https://www.youtube.com/watch?v=zYjKK0F3RDg&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=6

Industry40tv. (2022, agosto 2). *OPC UA PubSub: What it is and How it Works?* Retrieved from YouTube: https://www.youtube.com/watch?v=eTAK9noFHWE&list=PLIrJJXPVFRvjHsA9tta8yULOB8nPUO_G7&index=7

Mahnke, W., Leitner, S.-H., & Damm, M. (2009). *OPC Unified Architecture.* Springer.

Matyas, K., Nemeth, T., Kovacs, K., & Glawar, R. (2017, april 27). *A procedural approach for realizing prescriptive maintenance planning in manufacturing industries.* Retrieved from Google Scholar: https://www.sciencedirect.com/science/article/pii/S0007850617300070

Mondejar, J. A. (2023). Automatización Avanzada. ICAI Comillas.

NAMUR Open Architecture (NOA). (2021, december 5). Retrieved from Samson: https://www.samsongroup.com/es/actualidad/actualidad/detalles/news/fachwissen/namur-open-architecture/

NIST. (n.d.). *Cybersecurity Framework: Manufacturing Profile.*
NIST. (n.d.). *Cybersecurity Framework: Ransomware Profile.*

OPC Foundation. (2023). *UA-ModelCompiler*. Retrieved from GitHub: https://github.com/OPCFoundation/UA-ModelCompiler

Piromalis, D., & Kantaros, A. (2022, july 7). *Digital Twins in the Automotive Industry: The Road toward.* Retrieved from MDPI: https://www.mdpi.com/2571-5577/5/4/65

Pontarolli, R. P., Bigheti, J. A., Sá, L. B., & Godoy, E. P. (2023, january 27). *Microservice-Oriented Architecture for Industry 4.0*. Retrieved from MDPI: https://www.mdpi.com/2673-4117/4/2/69

Represa, J. G., Larrinaga, F., Varga, P., Ochoa, W., Perez, A., Kozma, D., & Delsing, J. (2023, january 31). *Investigation of Microservice-Based Workflow Management Solutions for Industrial Automation.* Retrieved from MDPI: https://www.mdpi.com/2076-3417/13/3/1835

SIEMENS. (2021, october). *SIMATIC IOT2050*. Retrieved from RS Componentes : https://my.rs-online.com/web/p/iot-gateways/2017732

Weis, O. (2019, december 17). *Interfaz de comunicación serie. Pinout RS232.* Retrieved from Virtual Serial Port: https://www.virtual-serial-port.org/es/article/what-is-serial-port/rs232-pinout/

Zonta, T., Costa, C. A., Righi, R. d., Lima, M. J., Trindade, E. S., & Li, G. P. (2020, october 6). *Predictive maintenance in the Industry 4.0: A systematic literature review.* Retrieved from Google Scholar: https://www.sciencedirect.com/science/article/pii/S0360835220305787