Belage Yogesh Suresh, B.E.

IIoT / Industrial automation / Communication systems (OPC-UA standard / specifications, use cases, solutions)

MASTER'S THESIS

to achieve the university degree of

Master of Science

Master's degree programme: Production Science and Management

submitted to

Graz University of Technology

Supervisor

Ass.Prof. Dipl.-Ing. Dr.techn. Norbert Hafner

Institute of Logistics Engineering

Graz, February 2022

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis.

Date, Signature

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen nicht benutzt und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche gekennzeichnet habe.

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Graz am…………………………… ……………………………………………

(Datum/Date) (Unterschrift / signature)

Foreword

Thesis focuses on the topic of ‘IIoT, industrial automation, communication systems by using communication standard OPC-UA’. This topic appealed to me ever since I first came in contact with it. The subject automation technologies for production systems introduced about OPC UA. My studies have allowed me to explore topic along with many directions that it comes with.

I would like to express my sincere gratitude to Ass.Prof. Dipl.-Ing. Dr.techn. Norbert Hafner for giving me opportunity, trusting, supporting, and supervising me through all this process. He was always available to answer my queries. His excellent guidance has allowed me to explore this topic.

I am incredibly grateful to all who have helped me. I am very thankful to my family for their unconditional support and understanding throughout all these years. My parents made it possible for me to follow the path that I wanted to follow. I would like to thank my friends who supported me during studies.

Belage Yogesh Suresh
Graz, February 2022

Abstrakt/Zusammenfassung

Diese Masterarbeit befasst sich mit industrieller Automatisierung mit Schwerpunkt auf industriellen Kommunikationssystemen unter Verwendung des Kommunikationsstandards OPC UA (Open Platform Communications-Unified Architecture) in Intralogistik- und Produktionssystemen.

‚Industrial Internet of Things' (IIoT)-Probleme werden durch den Einsatz von OPC UA-Standards gelöst. In der Industrieautomation sind Machine-to-Machine- und Machine-to-Cloud-, MES- und ERP-Kommunikation mit Hilfe von Totally Integrated Automation (TIA) möglich. Die in der Industrieautomation eingesetzten Kommunikationssysteme sollten über ein einheitliches Kommunikationsprotokoll verfügen, das durch OPC UA bereitgestellt wird. Mehrere Programmiersprachen als auch Komponenten aus verschiedenen Branchen und Betriebssystemen lassen sich mit OPC UA integrieren. OPC UA bietet eine unabhängige Kommunikation, Skalierbarkeit, Sicherheit der Datenübertragung, serviceorientierte Architektur sowie Lösungen für IIoT und Industrie 4.0. Die Spezifikationen für die industrielle Automatisierung im OPC UA-Standard konzentrieren sich auf statistische Daten und Stacklights. Die Integration von OPC UA und PROFINET mit Industrial Ethernet bieten Lösungen für industrielle Automatisierungsprobleme. PROFINET wird auf der Feldebene implementiert, z. B. bei Sensoren und Aktoren. OPC UA wird in der Steuerungsebene eingesetzt, z.B. bei MES und bei Anwendungen für die vorausschauende Wartung. OPC UA wird außerdem als standardisierte Schnittstelle für Daten verwendet, diese Möglichkeit wird von TIA bereitgestellt. Das TIA-Portal bietet durchgängige Workflows und Datenaustausch.

Industrial Ethernet erfüllt die Anforderungen der Automatisierung wie Echtzeitfähigkeit und hohe Geschwindigkeit. Drahtlose industrielle Kommunikation wird in der Intralogistik und in der Automobilindustrie eingesetzt. Die Kombination von PROFIsafe und PROFINET ist nützlich für die ausfallsichere industrielle Kommunikation.

Industrie 4.0 Anforderungen werden durch OPC UA Lösungen erfüllt. Die Anwendungsfälle und Lösungen von OPC UA bei Siemens werden in dieser Arbeit ausgeführt. Anwendungsfälle der Digitalisierung zeigen die Bedeutung von TIA, OPC UA. Im Bereich der Automatisierung werden OPC UA und PROFINET zusammen mit TIA eingesetzt, um das Konzept der Smart Factory zu verwirklichen. Die daraus resultierenden industriellen Kommunikationsprobleme können also durch den Einsatz von OPC UA Standard, TIA und PROFINET Technologie gelöst werden.

Abstract

The thesis consists of industrial automation with major focus on industrial communication systems by using communication standard OPC UA (Open Platform Communications - Unified Architecture) in intralogistics and production systems.

Industrial Internet of Things (IIoT) problems are solved by utilizing the OPC UA standard. In industrial automation, machine to machine and machine to cloud, MES, ERP communication are all possible with the help of Totally Integrated automation (TIA). The communication systems used in industrial automation should have a standard communication protocol, which is provided by OPC UA. Multiple programming languages, components from various industries and operating systems are possible to integrate by using OPC UA which means OPC UA provides independent communication. Scalability, security of data transfer, service-oriented architecture, integration with engineering such solutions for IIoT and Industry 4.0 are given by OPC UA. Industrial automation specifications in OPC UA standard are focused on statistical data and stacklights. The integration of OPC UA and PROFINET with Industrial Ethernet provides solutions for industrial automation problems. PROFINET is implemented at field level, such as sensors and actuators. OPC UA is used at control levels such as MES, applications for predictive maintenance. OPC UA is used as standardized interface for data and this facility is provided by TIA. The TIA portal provides continuous workflows and data exchange.

Industrial Ethernet overcomes automation requirements such as real time capability, high speed. Wireless industrial communications are implemented in intralogistics, automotive industry. PROFIsafe and PROFINET combination is useful in failsafe industrial communication.

Industry 4.0 requirements are fulfilled by OPC UA solutions. The use cases and solutions of OPC UA in Siemens are mentioned. Digitalization use cases prove importance of TIA, OPC UA. In factory automation, OPC UA and PROFINET are used with TIA to achieve smart factory concept. So, industrial communication problems are solved by using OPC UA standard, TIA and PROFINET technology.

List of abbreviations and acronyms

ADSL	Asymmetric Digital Subscriber Line
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
AR	Augmented Reality
ARM	Advanced RISC Machines
CNC	Computer Numerical Control
COM	Component Object Model
CPS	Cyber Physical Systems
CPU	Central Processing Unit
DSL	Digital Subscriber Line
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standard Institute
FCAPS	Fault Configuration Accounting Performance Security
5G	Fifth Generation
GSM	Global system for Mobile communications
HMI	Human Machine Interface
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IP	Internet Protocol
IPC	Industrial Personal Computer
IT	Information Technology
LAN	Local Area Network
LTE	Long Term Evolution
MES	Manufacturing Execution System
MQTT	Message Queue Telemetry Transport

M2M	Machine to Machine
OEM	Original Equipment Manufacturer
OPC- UA	Open Platform Communications – Unified Architecture
OT	Operational Technology
PC	Personal Computer
PCC	Processor Clocking control
PDO	Petroleum Development Oman
PLC	Programmable Logic Controllers
PubSub	Publisher / Subscriber
QM	Quality Management
RISC	Reduced Instruction Set Computer
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDO	Standards Developing Organization
SFC	Shopfloor Control Number
SHDSL	Single-pair High-speed Digital Subscriber Line
SOA	Service Oriented Architecture
SVG	Scalable Vector Graphics
TCP	Transmission Control Protocol
3GPP	Third Generation Partnership Project
TIA	Totally Integrated Automation
TSN	Time Sensitive Networking
UA	Unified Architecture
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network
WBM	Web Based Management
WEF	World Economic Forum
XML	Extensible Markup Language

Contents

1 Introduction

In this chapter introduction of thesis is given with background overview, its objectives, thesis structure.

1.1 Background overview

Technical advancements have been made in the domains of artificial intelligence, digital computing, and mobile platforms. Today's advancements are beneficial to both consumers and businesses. While this has aided companies in their digitalization efforts, as well as resulting in various businesses are incorporating new technologies into their operations.The base technologies used in industry 4.0 are Internet of Things, cloud, analytics and huge data.[1]

Organisations that develop well-built procedures and analyse how technology optimizes are more likely to implement a new technology successfully so that employees may perform their best work. Companies can respond to their customer needs in real time due to large amounts of data and the sharing of information across accessible networks. Nowadays in all industries like agriculture, automotive, medical etc. data transfer and processing are involved. Industry 4.0 is the latest and fourth phase of industrialization. Industry 4.0 brings many new opportunities and difficulties. The smart manufacturing concept is part of Industry 4.0. This help in production of customized products with high quality.[1]

The open standard OPC UA (Open Platform Communications – Unified Architecture) is used for industrial communication from M2M (machine to machine) and machine to cloud. It is platform independent and guarantees high security of communications. It meets requirement of time related applications. All automation levels are directly connected. It provides fast communications. As seen in [2], Holger Junker mentioned that “The only communication technology in the factory with implicit security features and the potential to meet the challenges posed by Industrie 4.0 that I am aware of today is OPC UA” [2]. Siemens is using OPC-UA combined with PROFINET to solve problems in industrial communication.[2]

1.2 Aim

Main aim of this thesis is focusing on industrial automation (production and / or intralogistics) by considering “pyramid of automation” (field to cloud) with OPC-UA standard as a solution for IIoT problems.

1.3 Thesis structure

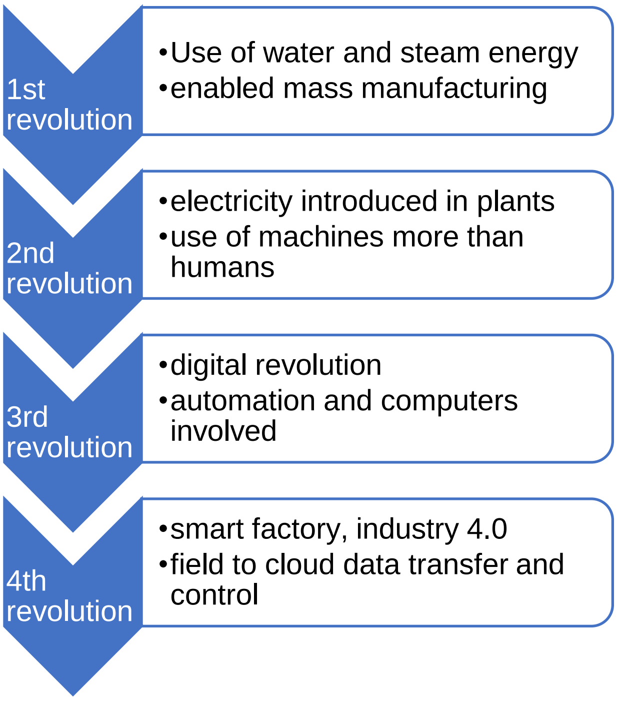
Thesis includes industrial automation in Siemens and OPC-UA. Siemens uses TIA (totally integrated automation) for industrial communication. Research on requirements and specifications of OPC-UA is important. Siemens is using OPC-UA in TIA portfolio. Also, PROFINET and OPC-UA will be combined in future for communication in enterprise digitalization. The use cases and solutions are mentioned to have knowledge about usage of OPC UA into industrial automation.

2 Literature review

In this chapter overview of industry 4.0 (components, advantages, and challenges) is explained. M2M (machine to machine) communication plays important role in industry 4.0.[3]

2.1 Introduction to industrial revolutions

People examined and created mechanical, electrical, and information technologies within the first three industrial revolutions in order to maximize the efficiency of industrial processes. In first revolution water and steam energy were used to achieve large production. Second revolution is also known as technology revolution in which electricity is used in plants to create production lines. From this stage machine use is increased. Little amount of automation was possible. Then third revolution came into picture which was digital revolution. Computers were used to monitor. Communication technology was developed for better communications during production phase. Here automation began and requirement of humans reduced. For implementing automation in processes PLCs were used. Major components in these revolutions were electronics involved, computerized processes and automation. Fourth revolution is referred as industry 4.0 which includes concept of smart factory. Data is collected from factory floor and send it to cloud with the help of information transfer. The Internet of Things (IoT) and M2M communications are being merged for improved automation, expanded connectivity and self-monitored systems.[3]



1st revolution
- Use of water and steam energy
- enabled mass manufacturing

2nd revolution
- electricity introduced in plants
- use of machines more than humans

3rd revolution
- digital revolution
- automation and computers involved

4th revolution
- smart factory, industry 4.0
- field to cloud data transfer and control

Figure 1: Industrial revolutions [3].

2.2 Industry 4.0 / Industrial Internet of Things (IIoT)

There are some basic components, advantages, and challenges in industry 4.0. To achieve target of smart factory these challenges should be solved. [3]

2.2.1 Design principles of industry 4.0

Design principles are discussed below.

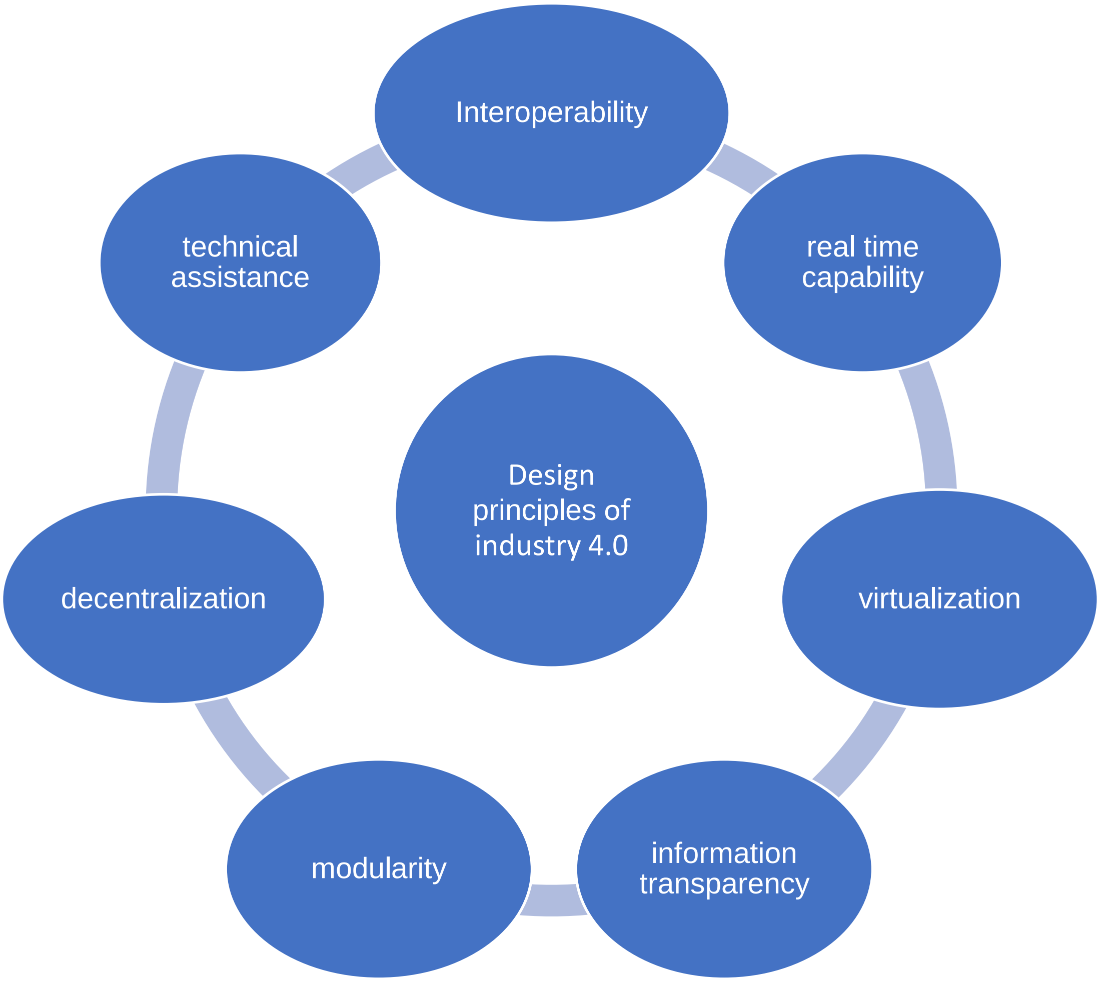


Figure 2: Design principles of industry 4.0 [3].

Interoperability

Interoperability plays an important role in optimizing process and production capability. Interoperability describes the capacity for items, computers, and people in the industry to communicate, exchange data, and coordinate their operations. Machines and workers can be easily connected. IoT is important for communication.[3]

Virtualization

By use of virtualization, financial savings can be done. Different physical resources are needed to build virtual resource.[3]

Decentralization

Transfer of data from saving to uploading is done by decentralization. Industry 4.0 is decentralized so that it can be used easily. All industries implementing decentralized plants which consists of new technologies.[3]

Real-time capability

All data operations should be done with real timing so that obtaining data at any time is possible. If some problem arises then from real time system, problem can be observed and solved easily. Also, there is good scope for development. Processes can be optimized and made cost effective.[3]

Modularity

Modularity is capacity to adapt changes in industry such as wants and expectations. A business split in tiny and well-defined groups that concentrate on key market components.[3]

Information transparency

Transfer of information from shop floor give clear idea to achieve excellent results. More profit generation is possible with large amount of data and information. Data collection at different production steps is important to increase productivity.[3]

Technical assistance

It is used for handling important challenges as soon as possible and getting smarter decisions. It lowers number of workplace accidents.[3]

2.2.2 Industry 4.0 components

There are some basic components of industry 4.0 such as cloud computing, Internet of Things, cyber physical systems, cyber security, data analytics etc. In cyber physical system, physical process is controlled by computerized networking system. RFID generally uses electrical field to differentiate things by using tag. Integration of sensors and actuators is essential to computer functions.[3]

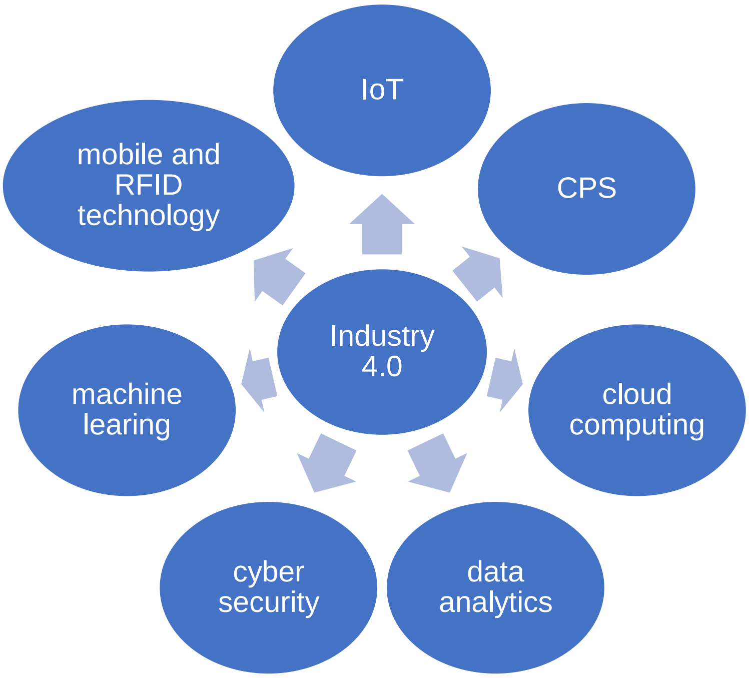


Figure 3: Industry 4.0 components [3].

Technology, distribution network, production, sales activities, automation and business connectivity and integration are all required for smarter manufacturing. This facilitates cloud. Furthermore, typically large amount of data saved and evaluated is analyzed simply and price effective on cloud. This will decrease initial costs and allowing them to meet needs and grow.[3]

Internet of things is an important factor. Machines on the shopfloor have IP addresses and sensors that facilitate interaction with other internet PCs. This link enables the collection, analysis, and exchange of large amounts of relevant data. As a result of Industry 4.0, businesses may now create digital twins, which are computerized duplicates of systems, production lines, warehouse, and supply networks.[3]

Artificial intelligence and deep learning will be capable to see, forecast and automate marketplaces and business tasks. Predictive maintenance is possible with algorithms.[3]

Most of companies not taking cyber security issues seriously. But cyber-attacks can destroy total manufacturing inside of plants.[3]

2.2.3 Advantages of industry 4.0

The major benefit is that it improves efficiency in manufacturing plant. In smart factory several smart devices are self-optimizing the production operations. This is especially important for sectors that use high end expensive manufacturing machinery like semiconductor companies. Creating customer-oriented atmosphere which facilitates customers to simplify and efficiently satisfy requirements. As a result, gap in producer and client is narrowing. Both parties would communicate with each other instantly. The objective of industry 4.0 is to establish the real-time connections between people, goods, and machinery during production processes. This speed up supply chain process.[3]

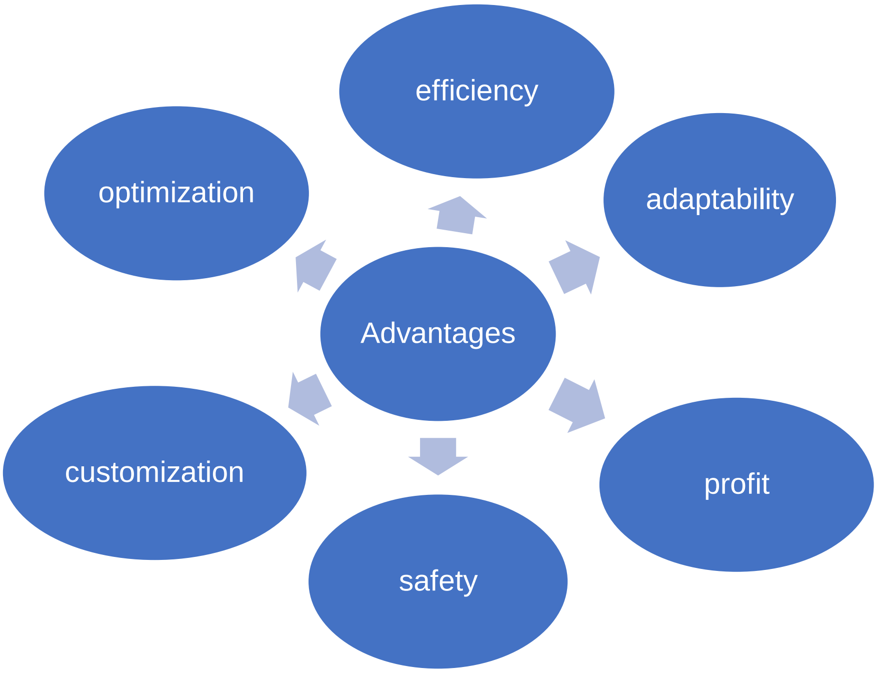


Figure 4: Advantages of industry 4.0 [3].

2.2.4 Challenges in industry 4.0

Employment issues will rise because of automation in manufacturing processes. There are lot of technical challenges such as hardware and software required. Implementation of new technology is costly. Finding and developing a new technology also need time. In this industry collection of large amounts of data is needed, so may be some consumers will not allow to use their data in companies. It is impossible to work in smart factory without data.[3]

2.3 M2M communication

M2M is potential technology for communicating systems. In M2M huge number of smart devices communicate without physical involvement of human. M2M in used in different industries like medical, industry automation, domestic networks, transportation. Decisions are taken automatically. Time is well managed with all automatic devices. Costs can be reduced. Interoperability helps in combining current and future technology. Protection of data is important. Challenges like reliability, energy efficiency, service quality should be solved. For achieving sustainability, standardization plays an important role. Standardization speeds up the development. There are some organizations like 3GPP, ETSI, IETF and oneM2M which are developing standards. Standardization efforts are also taken by technology driven alliances (WiMAX technology, Wi-Fi alliance, Zigbee alliance, Bluetooth technology) and application driven alliances (telecommunication industry association, international telecommunication union, home grid forum, open mobile alliance, digital living network alliance etc.).[4]

There are new challenges such as new protocol design, data collection and energy efficient operations. The data route from machine nodes to outer environment is controlled by protocols.[4]

OPC UA and Industrial communication

The data collection is needed from every element in automation systems for achieving Industry 4.0 concept. The OPC UA standard allows collection of data from sensors, actuators by using control technology. This collected data from field level is shared to cloud level. The industrial communication is focused on real-time capabilities. The company HMS Industrial Networks has compared data from 2016 and 2017 for analysing use of industrial networks. The fieldbuses have 4% of growth rate, and Industrial Ethernet has 22% of growth rate. The wireless networks are growing with 32% of growth rate.[5]

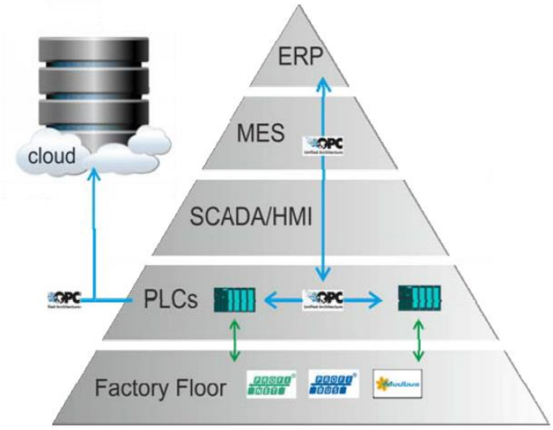


Figure 5: OPC UA vertical and horizontal integration [5].

The OPC UA is used in horizontal communication like PLC-to-PLC communication and vertical communication from PLC to upper levels such as ERP. The vertical integration also includes communication between PLCs and cloud. OPC UA is used not only as a protocol but also as a framework for the exchange of data. The exchange of data in OPC UA is carried out by two mechanisms which are client-server and PubSub. These two communication mechanisms are explained in detailed in the thesis. High speed manufacturing with high efficiency is a result of interoperability of various systems from different manufacturers.[5]

3 Industrial automation in Siemens

Industry is in the beginning of industry 4.0. The digitization of manufacturing is being followed by automated processes. The objective is to boost productivity, quality, efficiency etc. In the sector of automation Siemens is offering automation technologies and digitization of manufacturing. Siemens has unique portfolio for automation. It has industry software, services for digital enterprise, industrial controls, industrial communication, locating and identification systems, automation systems, process instrumentation, process analytics, PC-based automation, control and monitoring systems, power supplies.[6]

3.1 Totally integrated automation (TIA)

The TIA is combination of software, hardware, services, IT and OT, and growing future technologies. The portfolio expands to meet varying needs and allows innovative opportunities in business. Many industries are making a comeback in TIA platform. Edge devices now have adequate computational capacity to execute specific programs and organize communication with other portions of the plant, therefore IT technologies are transferring to the industrial sector. Various services ranging from advising to installation and optimization, round out the package, assisting machine builders and machine operators in uncovering latent optimal solution possibilities.[7]

Siemens started integrated engineering, communication, data management 25 years ago. Now in manufacturing industry, production processes (OT) and office management (IT) are linked with each other by using TIA. TIA focus on productivity and efficiency. Everyday new technologies are coming in the market but TIA from Siemens providing solutions and added value to customers. For having digital enterprise, TIA is the solution. Companies creates big quantity of data but sorting this data to useful data is important. Digital enterprise combines real and digital environment.[8]

3.1.1 Integration- integration of services, software and hardware

The Integration[1] is integration of services, software, and hardware. This integration provides solutions for automation in various industries. The production processes are more dependent on IT systems. The combination of IT technologies with production is possible with this integration. The services are available for implementation, consultation. The optimization of plant also included in services. The overall process of integration provides security, engineering solutions, data intelligence.[7]

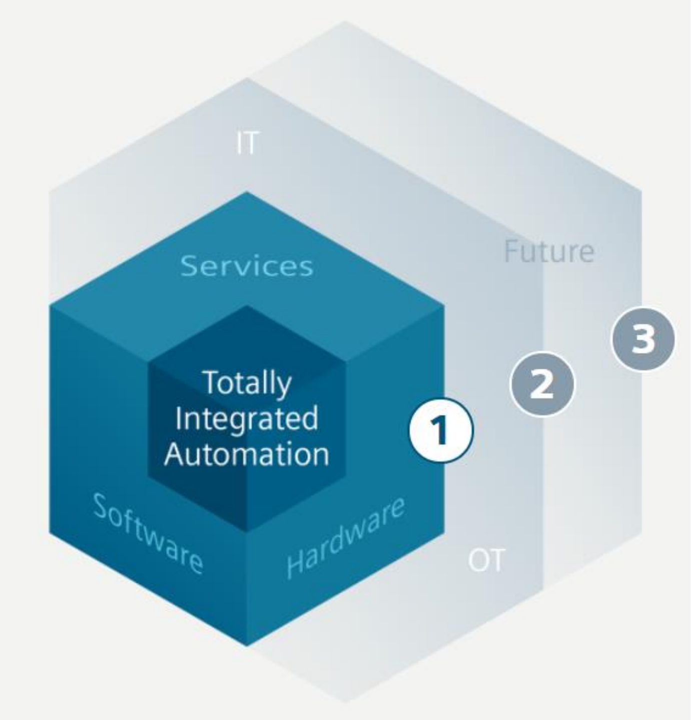


Figure 6: Seamless integration of hardware, software, and services [8].

TIA portfolio

It is used in various industries. All components are linked together. TIA is divided into two major technologies. One is operational technology and other is information technology.[7]

It provides automation solutions to different industries through its comprehensive approach towards designing. It also considers communication standards and safety. Data intelligence consists of modern technologies such as artificial intelligence to convert data into knowledge and provides transparency. In Siemens data intelligence is provided by MindSphere, SIMATIC RTLS, SIMATIC SCADA System, Industrial Edge.[7]

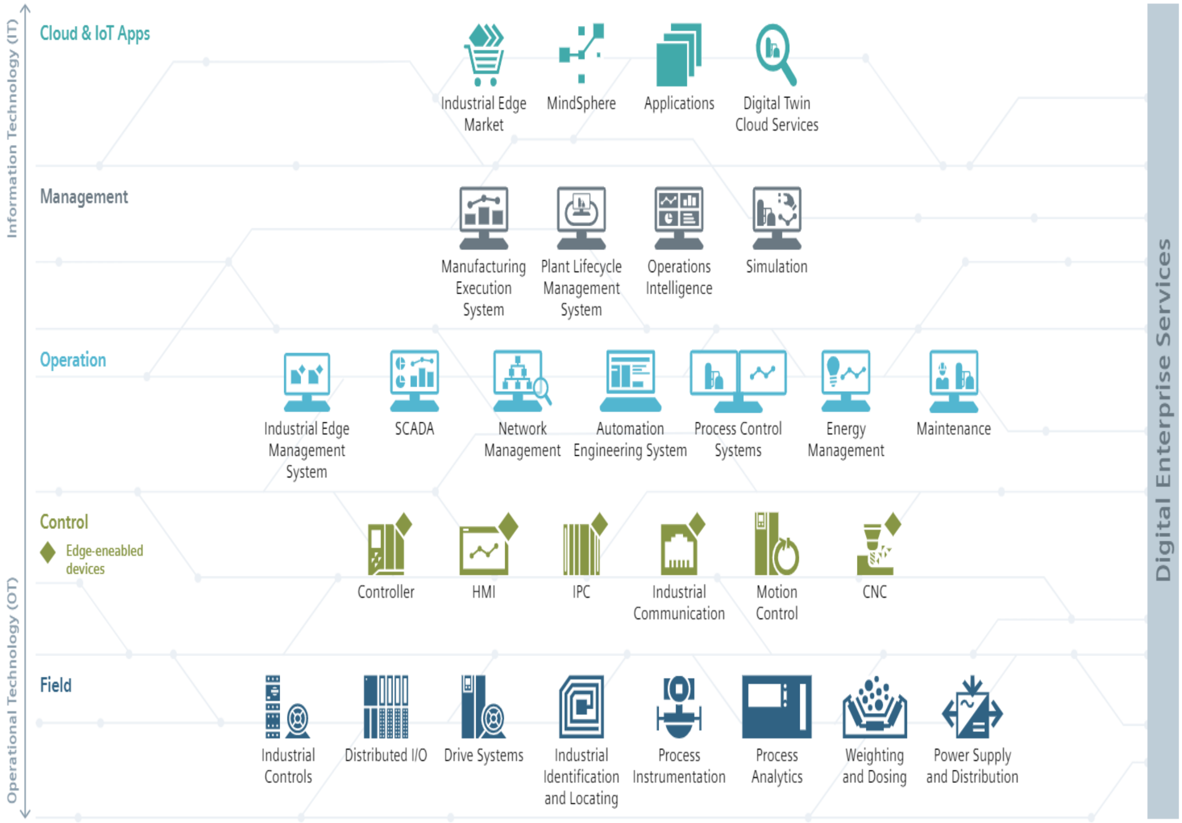


Figure 7: TIA portfolio [7].

TIA has consistency with strong communication networks. For vertical and horizontal communication there are platform independent standards. TIA consist of industrial security to ensure plants, machines etc. are safe. Safety is integrated in TIA to ensure and protect plant, human, machinery and environment.[7]

3.1.2 Integration- vertical and horizontal integration

It consists of horizontal and vertical integration. TIA provides connectivity which connects field and machine levels horizontally. OT and IT are vertically connected. From shop floor to top floor automation is integrated.[9]

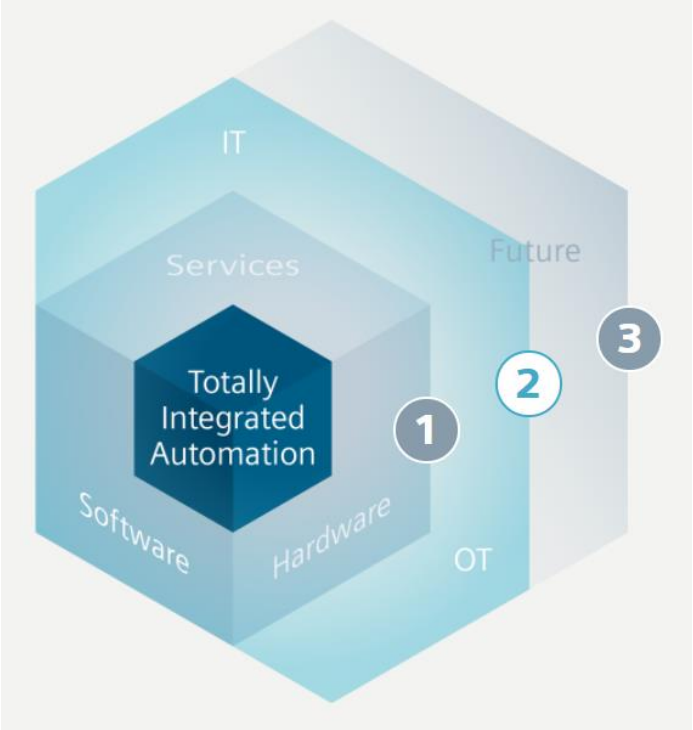


Figure 8: Comprehensive horizontal and vertical integration [8].

From OT to IT with TIA

Technical specifications of machines and production line such as communication standard, machine functions should be known. Machine producers use specifications to produce ideal machine idea. Interdisciplinary engineering implies working on automation, mechanical and electrical simultaneously. The aim is to know about how all things work virtually without producing real machine. After building machines, integration of machines is done. Standardization and data models help in line integration. OT-IT integration connects total shop floor to management level. Then from huge data generated, useful data is extracted. Data is up to date because of TIA.[9]

3.1.3 Integration- integration of future technologies

TIA integrates future technologies such as autonomous systems, artificial intelligence, 5G, augmented reality.[8]

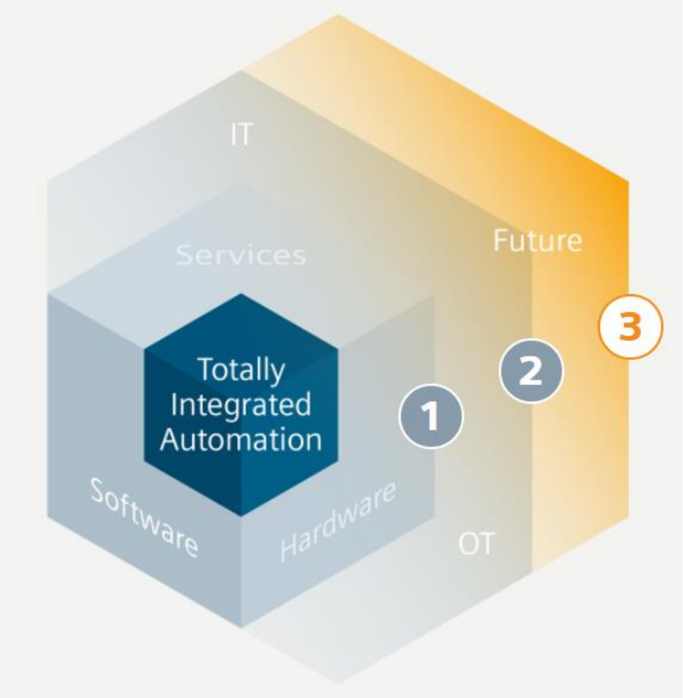


Figure 9: Step-by-step integration of future technologies [8].

The utilization of AI makes handling of information simpler, quicker, and more exact. AI in SIMATIC helps to get image-based Al solutions. Higher product quality is obtained by use of AI in quality assurance with SIMATIC S7-1500 TM NPU AI module. Digital simulation is easy with AR.[10]

3.2 Control technology

This section includes industrial communication, IPC, HMI, controller, motion control, CNC [11].

3.2.1 Controller

The SIMATIC controllers not only have high strength hardware but also, they have new functions. In automation processes, controllers are used. They are important component of OT/IT integration and TIA.[11]

Controllers are used to integrate lines for optimum data exchange. For removing confusion between machines OPC UA communication standard is used. In Siemens, PROFINET and OPC UA are used together [11].

The functioning and construction of automated systems are becoming increasingly sophisticated because of automation and production flexibility [12].

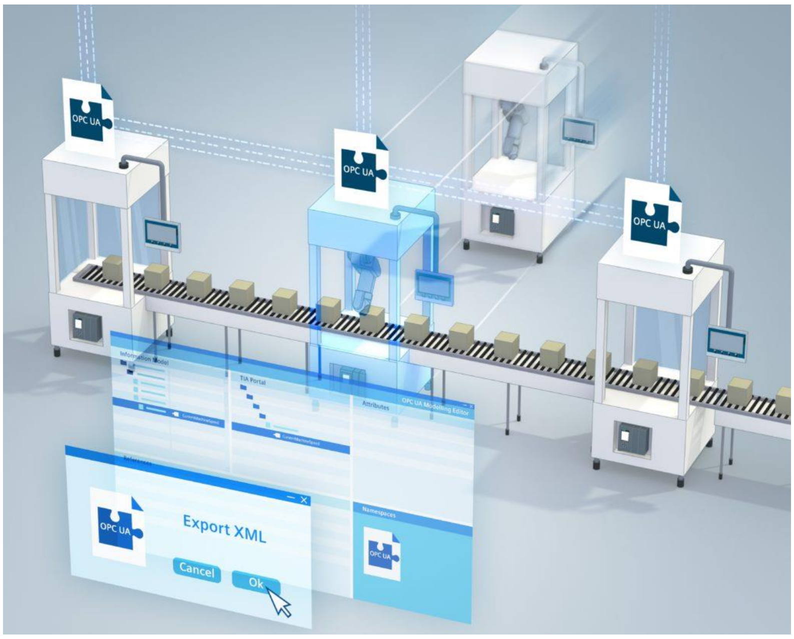


Figure 10: Line integration [12].

Standardization of communication between production machines and higher IT systems is necessary for smooth communication. By use of plant simulation, performance of lines is increased. Connection of SCADA with MES and IT is done with WinCC Unified to use as platform for manufacturing line. Plant operator includes line planning and virtual operator training. Line integrator consist of implementing line control, virtual validation of the line control.[12]

3.2.2 SIMATIC HMI

To control and monitor different systems, human machine interface plays an important role in efficient integration. SIMATIC WinCC Unified is a totally new perception framework that empowers you to effectively dominate the difficulties of digitization in machine and plant designing. It runs anywhere and anytime. It is simple to use and scalable. TIA portal can be visualized with WinCC efficiently.[13]

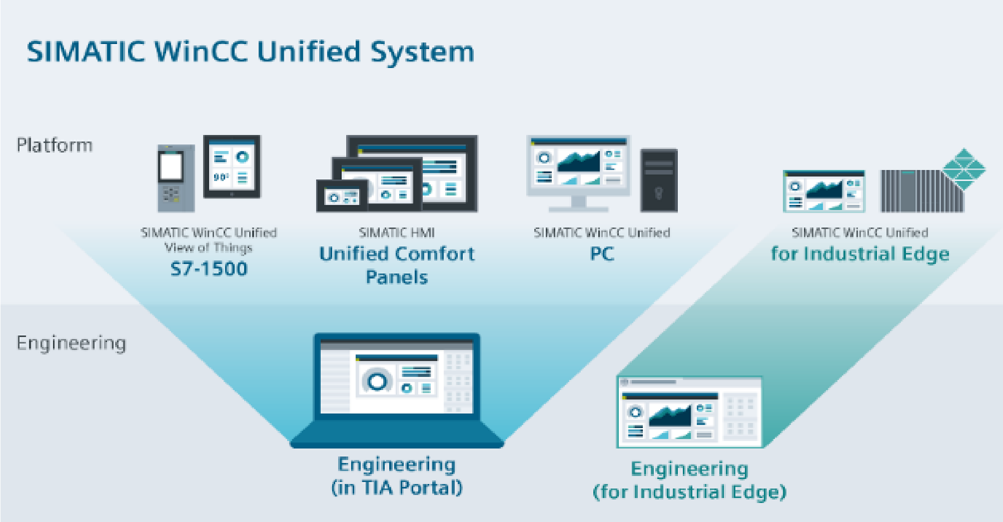

SIMATIC WinCC Unified System
Platform
SIMATIC WinCC Unified View of Things
S7-1500
SIMATIC HMI
Unified Comfort Panels
SIMATIC WinCC Unified
PC
SIMATIC WinCC Unified
for Industrial Edge
Engineering
Engineering (in TIA Portal)
Engineering (for Industrial Edge)

Figure 11: SIMATIC WinCC unified system [13].

Why WinCC unified system is unique?

JavaScript, HTML, and SVG are used in user interfaces. So only updated browser is needed for visualization. There is no need of extra apps. JavaScript gives functions which are in this language to WinCC. SVG graphics provide required quality of image. It supports both static and dynamic graphics. WinCC is open for extensions and easily connected to IT system. It is possible to integrate it with OPC UA. Reports are extracted in different forms. Alarming is included to take instant actions against failures and errors.[13]

Basic panels are used in basic HMI. In advanced HMI not only comfort and mobile panels but also PC based panels are used. If application complexity is high, then advanced HMI is used to increase system performance. Efficient engineering, innovative design, safety etc. are some performance factors. In less time development of visualization is possible. Rapid commissioning is used to detect errors and analyse errors. SDS tec GmbH Germany has specialized in biogas and cabinet design. SIMATIC HMI, TIA portal, and WinCC are used in this company which provides opportunity to integrate different ideas. Steritech S.A. France is automated company to produce autoclaves, where SIMATIC WinCC and Trilogy provided visualization solutions with touch display.[14]

Development of SIMATIC HMI software is going on to create more transparency, flexibility, and openness. SIMATIC WinCC Professional is the SCADA system which is used with TIA portal. It gives information about machines, production process flows, plants. It increases usage of manufacturing facilities, decrease costs. WinCC WebUX helps in controlling of plant by use of internet. Phones, PCs, tablets can be used to operate and monitor. Any information related to plant is available whenever needed. Due to implementation of different languages, this software is possible to use in world. Because of this international teams can easily work together. There are lot of possibilities to show data such as historical data, current data. If there are dangers due to some reason, then these dangers are identified in early stage and then actions to overcome dangers are taken. It can be used in all types of industries. Reporting based on web is done to convey information to managers and quality team. With the help of standards, it has more openness and simple integration. Vertical integration and cross vendor communication are included in this software. Visualization is done automatically depending upon code.[15]

SIMATIC WinCC V7 is used for maximum production efficiency and plant transparency. Mass data is efficiently processed. It is used worldwide because of multiple language. It has modern system for graphics. Components used in projects are in standardized picture form. It has some similarities with WinCC Professional such as efficient problem solving, data management, reporting based on web, message analysis. It has some extra features such as functionality which is based on calendar and event. It analyses performance for optimization. There is possibility to use this software in tablets and mobile phones. Mobile SCADA has advantages such as user get information in very less time, less costly, it is focused on target.[16]

SIMATIC WinCC OA is used for huge and complex processes. It is available on Android, iOS, Linux, and Windows. It provides safety in communication. It has high openness and flexibility. It is platform independent and has benefits in worldwide businesses. It is best choice for systems that are broadly spread.[17]

3.2.3 SIMATIC IPC System

Industrial PC is used to control complicated tasks and provide data server. It solves the problems in automated factory. By using SCADA less time is needed to bring parts to the market. Test and validation also save time. Brilliant error tracking system decreases downtime. Preventive maintenance can be possible. Redundancy provides data, system availability. It gives high security. The mobile tablet PC helps not only in manufacturing processes but also in warehouse, plant maintenance. IPCs are used in image processing in industry, and it provides quality inspection. Production is connected to digital system. All processes generate data, this generated data is converted into information. IPC systems are available in different types of configuration and easy integrations are possible. It provides planning for future and in all environmental conditions there is guarantee of system availability. They reduce labor cost up to 60%. They have high scalability, ultra-compact shapes, optimum battery management.[18]

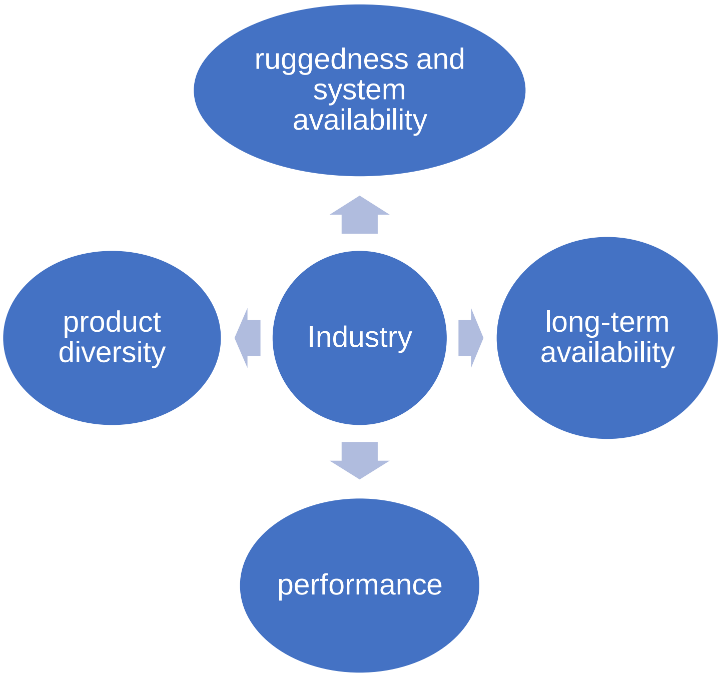


Figure 12: Advantages of SIMATIC IPC system [18].

3.2.4 Industrial Communication

Industries have different components such as workers, machines, production processes, energy management. Industrial communication is necessary to operate machines and to control power. OT and IT must work smoothly to make the best use of data obtained during production process. The optimization of automation elements is achieved. SCALANCE and RUGGEDCOM network components are used in planning and implementation phase. Main areas are industrial ethernet, rugged communication, wireless industrial communication, remote industrial communication, industrial network solution, network management. All these areas are explained in detailed in further part of this chapter. OT networks should be reliable and always available so that in all conditions data must be transferred. Failures can cost lot of money and speed of data transmission is focus of IT network. Industrial communication is needed in various industries like oil and gas, logistics, production, transportation. There are communication standards and platforms for smooth interaction between system and networks. OPC UA has open platform for digitalization while PROFINET is one important industrial ethernet standard used in digital factories. For example, in metal industry working temperatures are very high and quality of final product is important. So, network must be designed in such way that it should handle extreme situations in mill. The other example from logistics is AGVs need to travel in manufacturing hall. Therefore, network should provide real time communication with data security. In example of production network 4.0, communication network should provide central management, transparency in maintenance, fast diagnostic.[19]

3.2.5 Motion control

Only one CPU is used for managing various technical activities such as signal control, motion control. SIMOTION with motion controller gives high flexibility and performance for motion control functions such as path interpolation and distributed synchronous operation. Motion control functions efficiently operate multiple and single axis systems without requirement of any special programming skills. It processes signals at high speed and gives instant response which ensure high productivity and quality. The focus is on making single system for example only one controller or one engineering.[20]

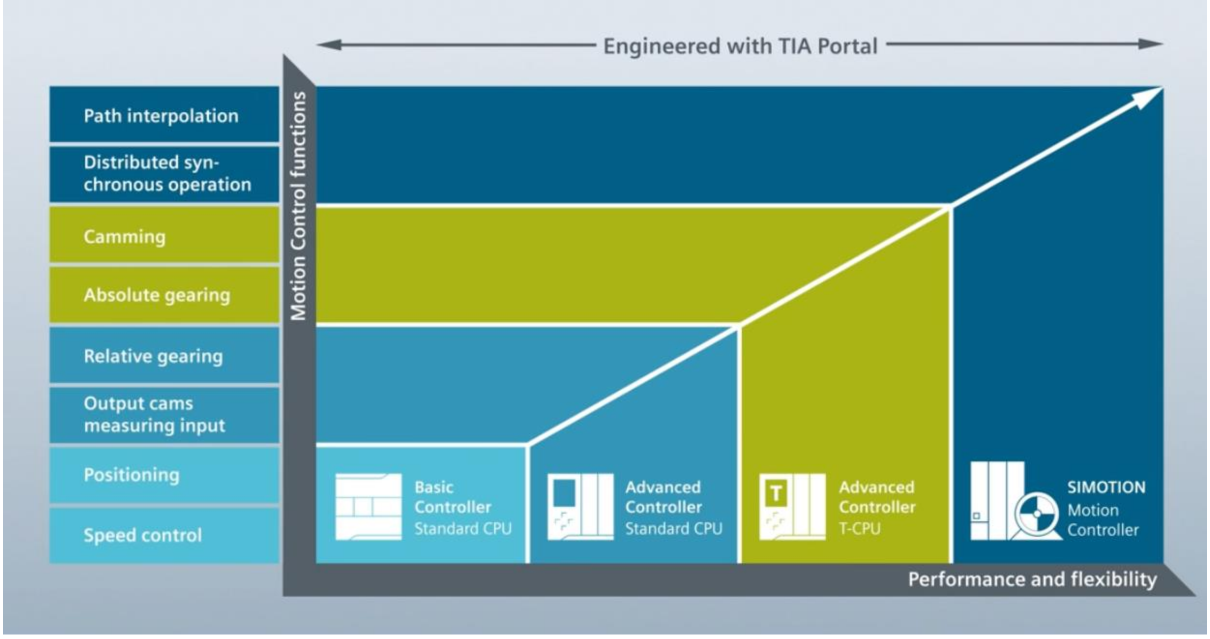

Engineered with TIA Portal
Path interpolation
Distributed synchronous operation
Camming
Absolute gearing
Relative gearing
Output cams measuring input
Positioning
Speed control
Motion Control functions
Basic Controller Standard CPU
Advanced Controller Standard CPU
Advanced Controller T-CPU
SIMOTION Motion Controller
Performance and flexibility

Figure 13: SIMATIC technology [20].

SIMATIC and SIMOTION controllers are responsible for solutions in motion control. Gathering of machine date help in predictive maintenance which can avoid failures.[20]

3.2.6 CNC

SINUMERIC offers manufacturing processes such as grinding, turning, additive manufacturing, milling in one machine. It gives programmes for parts with flexibility. It identifies loading condition during operations and controls feed rate to protect tools. It has friendly, self-explanatory user interface which is easily learned by new employees. CNC software for shopfloor provides minimum required power to operate machine. Tool systems has industrial solutions that are utilized in the automobile, aviation, electronics, and power production sectors worldwide. SINUMERIC equipment shows not only stability during performance but also reduces cost because less time is required for setup [21]. There are different CNC systems are available such as SINUMERIC MC for special technology, SINUMERIC 808 for basic machinery, SINUMERIC 828 is compact class, SINUMERIC 840 premium class and SINUMERIC ONE is also premium class for future.[22]

3.2.7 Failsafe control technology

Safety is important in automation plants to prevent machines, people and plant. The safety is important for automation systems, drive technology, industrial control technology, communication, controlling and monitoring. For failsafe automation systems, SIMATIC Safety Integrated and SINUMERIC Safety Integrated provide safety functions in software and hardware. SINAMICS drives have installed safety technology for failsafe drive technology. Control technology from Siemens provides safety by using SIRIUS Safety Integrated. SIMATIC HMI offers solutions for safety from basic to advanced level.[23]

Machine safety is effectively linked to the SIMATIC automation system with SIMATIC Safety Integrated. There is no need of separate system due to built in safety functions. So, no extra money required for engineering and hardware. The SIMATIC Safety Integrated consists of single communication, single controller, singles engineering. TIA portal supports integration of safety into already existing systems, communications.[24]

SIMATIC controllers have safety functions already integrated into them. The failsafe S7-1500 controllers have safety functions. They connect PROFINET and PROFIBUS to PROFIsafe devices. PROFINET is used to collect various signals and safety signals. Troubleshooting messages are directly shown on status display. Failsafe program is protected with extra passwords. For failsafe automation, various I/O systems are possible to integrate with SIMATIC ET 200.[25]

SIMATIC HMI has various safety solutions such as SIMATIC HMI key panels for basic HMI, SIMATIC HMI mobile panels for advanced HMI panel based. The stop button for emergency is included in SIMATIC HMI mobile panels. These mobile panels can be connected with

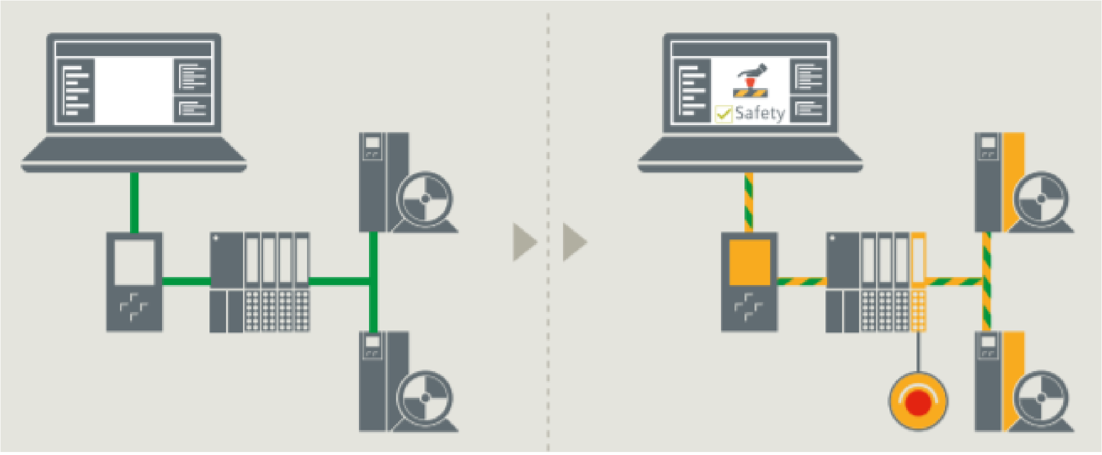


Figure 14: Easy integration of safety via TIA Portal [25].

PROFINET and TIA portal. SINAMICS converters are provided with functions of integrated safety and these functions fulfil requirements of drives with variable speed according to standard IEC 61800. Easy communication is possible with PROFIsafe by using PROFIBUS or PROFINET.[25]

3.3 Industrial communication

In digital industries, communication networks must provide high-speed transfer of data generated with security. Communication between OT and IT must be good. Based on expert structure development and execution utilizing RUGGEDCOM and SCALANCE network related components, industrial communication portfolio enables the appropriate networking of automation components. Siemens assists in laying an ideal basis for digitization and support throughout the digital transformation process with comprehensive range of industrial network technologies. Siemens consulting experts help to plan, create, and optimize networks with professional services for industrial networking. Specialized training programs are available to teach and certify staff so that they can continue to support and expand company's network. Siemens´s entire line of industrial communication devices and software satisfies all performance, reliability, robustness, and availability requirements. Siemens´s trained and experienced partners can provide additional, personalised help wherever in the world.[19]

3.3.1 Industrial Ethernet

The Industrial Ethernet is foundation for effective automation. As the world becomes more digital, the demands on industrial communications networks are growing. Communications networks that are powerful, integrated, and increasingly real-time competent are required. Industrial Ethernet, along with TSN (Time-Sensitive Networking) which is based on Ethernet standard in the coming years, is the tried-and-true technology to overcome challenges.[19]

Industrial ethernet can be customized to fulfill the needs of industries. Network components are designed in such a way that they can handle all types of environments. Industrial ethernet is designed in such a way that the wiring system is used directly at the workplace at high speed, has a strong backup plan if failure happens, and an alarm for continuous tracking of components involved in networking. The most difficulties in industrial automation are achieving reliable and efficient digitalization so that plant efficiency may be optimized by utilizing the advantages of edge and cloud-based applications. Traditionally, OT and IT were created and operated separately from one another, but they are now more convergent. Today's challenge is to link the field and control levels all the way to the cloud while taking use of current solutions strengths and forming new synergies. Siemens achieves this by merging two well-established standards: PROFINET for speed and reliability and OPC UA for data semantics and flexibility. Industrial ethernet is combination of hardware and software.[26]

a) Industrial ethernet switches

SCALANCE X switches are used in industries. In table switches are explained for various applications. Portfolio of switches explained in table with basic uses. There are eight major types of ethernet switches available, and they are again divided into different types.[27]

compact switch modules (CSM)	simple integration of machine, industry standard, less space required, easy to use
SCALANCE X-000 compact switches	used for small networks, plastic or metal used in housing, 5 to 8 ports, robust structure
SCALANCE X-100 unmanaged media converters and switches	used near the machines, 8 to 24 ports, signals conversion from electrical to optical
SCALANCE X-200 managed Gigabit switches	for variety of applications, robust, flexible, maximum 24 ports
SCALANCE X-300 rack mounted Ethernet switches	compact structure, flexible, up to 28 Gigabit ports

SCALANCE X-400 managed layer 2 switches	possible to create networks, transmission rates are high, port extenders are available
SCALANCE X-500 managed layer 3 switches	52 ports, transmission rate 10 Gigabit, central component of networks
SCALANCE X for process automation	used with PROFINET, use in control cabinet, for processes with huge data

Table 1: Types of industrial ethernet switches [27].

Advantages of industrial ethernet switches

SCALANCE X switches provide 10 Gigabits of transmission rates, and they have a huge number of ports. Installation is possible right at point of need. In the design of networks, high flexibility is possible. SCALANCE X-000 and SCALANCE X-100 product lines include the perfect unregulated switches if you require a low-cost alternative for easy networking of machine or little optical or electrical Ethernet networks. Versatile and powerfully managed switches from layer 2, SCALANCE X-300 and X-200, are the appropriate choices for applications which are machine oriented and networking systems in ring, line, and star structures if there is need of high network availability and have higher standards in terms of functionality and design. Layer 3 and layer 2 switches for big networks, the SCALANCE X-500 and X-400, provide maximum flexibility and network availability.[27]

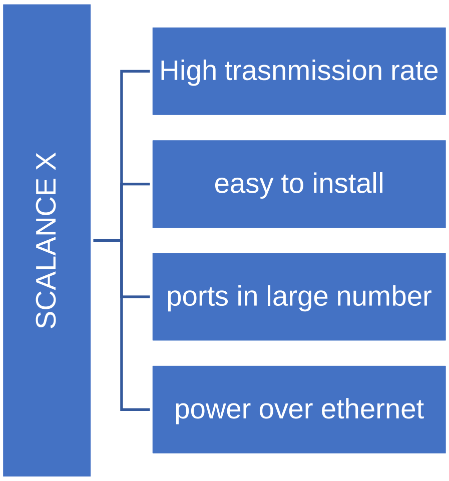


Figure 15: Advantages of industrial ethernet switches [27].

First example, SAPA Extrusion from Germany, a manufacturing company used SCALANCE X-300 ethernet switches for consistent production. Expansion in production is possible whenever required, and availability is increased because of the XR-300 switches. Communication is done via PROFINET and PROFIsafe to avoid troubles.[28]

Second example, Karl Simon GmbH and Co. KG from Germany, a metal working company. Simon's new production network is built around an industrial ethernet ring to which 32 SCALANCE XR524 switches are redundantly linked. Simon employs the SINEMA Server software for administration and troubleshooting. Simon employs the SCALANCE S615 Industrial Security appliance to link the subordinate plants, which each have their own plant network. As seen in [29], David Huber said that “In many production areas, for example in the sintering plants, we’re dealing with harsh environmental conditions. Thanks to the extended temperature resistance of the SCALANCE components, we’ve no problems with that” [29]. So, communication is secured and powerful with transparency.[29]

b) IoT Gateways / Devices

To take advantage of digitalization, cloud applications are must. Existing facilities may be readily connected to several cloud systems that use the standardized MQTT protocol, such as the MindSphere, using the Industrial IoT Gateways SIMATIC CloudConnect 7. CloudConnect connects sensors to cloud. Industrial IoT gateways SIMATIC CC712, SIMATIC CC716 have cloud interface type as industrial ethernet and protocols device interface as S7, OPC UA, etc. OPC UA server, and OPC UA client connections are possible with field devices.[30]

c) System interfacing

The IIoT and the required data streams necessitate an infrastructure capable of smooth vertical and horizontal data sharing that means networks with high performance. SIMATIC NET provides a wide range of communications processors for industrial PCs, distributed controllers, PCs, advanced controllers and basic controllers.[31]

d) Cabling technology

FastConnect assembly provides simple, fast, and correct connections. It is made up of tools, connectors, and cables, it is used not only in PROFINET, Ethernet but also PROFIBUS. Advantages of this technology are such as simple connections save time, color coding is used for no errors, designed by using international standards. Categories are copper cables and connectors, fiber optic cables and connectors, power cables.[32]

e) Network diagnostic

In SINEC NMS network management is done efficiently which is required in Industry 4.0. The advantages are that faults are quickly identified, all network components are monitored, and security management is performed. FCAPS (fault, configuration, accounting, performance, security) model is supported by SINEC NMS. Through OPC UA, data is transferred to other systems such as HMI.[33]

3.3.2 Network security

Industries must be protected from cyber-attacks to survive in the market. Network security provides protection against unauthorized connections. Based on the Industrial Security Standard IEC 62443, Siemens delivers solutions in the form of defense at all levels. With Zero Trust principles, the "Defense in Depth" idea may be enhanced. It is feasible to build extensive yet secure OT networks with the help of expert planning, design, and implementation of powerful network infrastructures.[34]

VPN employs encryption and authentication to ensure network security during distant communication. A firewall regulates data flow and prevents illegal data transmission. Plant segmentation is beneficial in terms of protection and lowering the chance of plant failure. Industrial firewall appliances with firewall rules up to 1000 and 600 Mbit/s throughput provide various firewall techniques to secure even flat networks. A strong Industrial VPN Appliance may support up to 120 Mbit/s throughput and maximum VPN connections 200, in addition to the firewall measures. Integration of the TIA portal with the firewall and VPN allows for quick and simple engineering.[35]

SCALANCE S is used in industrial networks and machines for security. Industrial firewall appliance and industrial VPN appliance are two categories of SCALANCE S. The TÜV has certified the SCALANCE S Security Appliance series to the Industrial Security Standard IEC 62443-4-1. These devices enable setups through CLI, Web-based management (WBM), and TIA portal, and may be linked through software for network management SINEC NMS. They also guarantee the installation of a configurable security zone by utilizing isolation of network or remote maintenance security. They're also suitable for temperatures ranging from -40 to +70 degrees Celsius.[35]

Appliances for industrial firewall have a firewall performance around 600 Mbit/s and use a bridge firewall to provide safe access across distinct network segments. Temporary network access can be allowed as needed thanks to user-specific firewall rules. For long distances, the connections are provided by Ethernet ports 10/100/1000 Mbit/s or fibre optics up to distance of 200 km. In a PROFIsafe environment, the firewall appliances in industries may also be utilized for isolation of network. SCALANCE SC636-2C, SCALANCE SC632-2C, SCALANCE SC622-2C are firewall appliances.[35]

The connection may be established via Ethernet connections with speeds of 10/100/1000 Mbit/s, as well as fibre optic cables over long distances (up to 200 km). 200 VPN connections are possible with maximum data throughput 120 Mbit/s. Different VPN appliances are available such as SCALANCE S615, SCALANCE SC646-2C, SCALANCE SC642-2C.[35]

Use case of network security

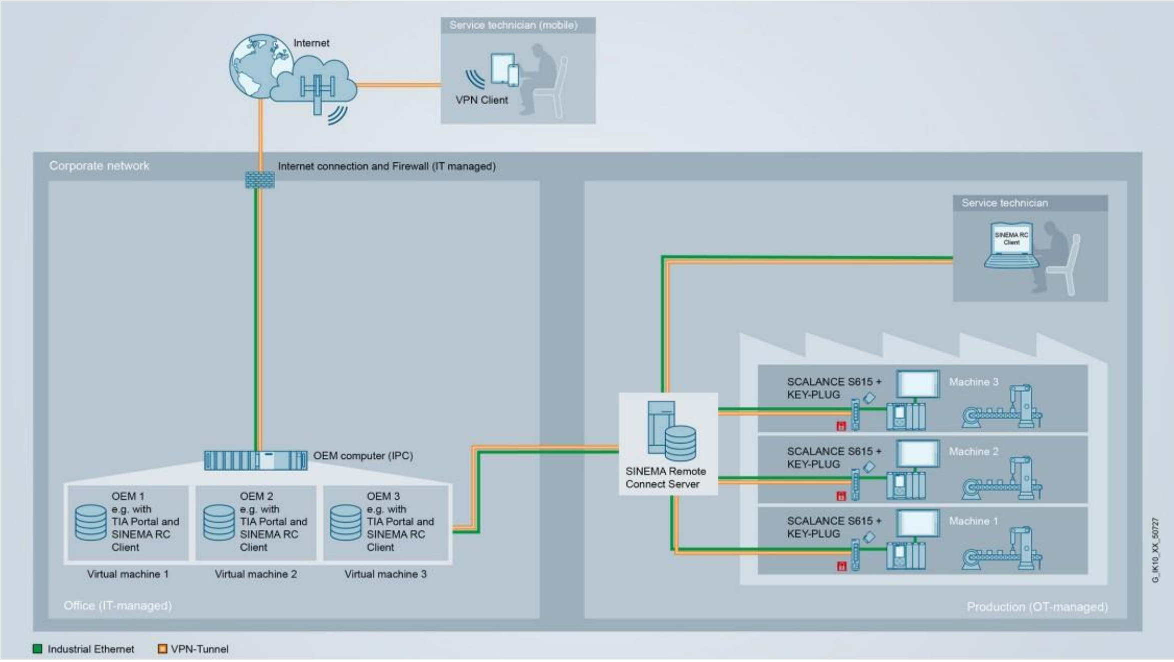


Figure 16: Remote connect server SINEMA and SCALANCE S615 in enterprise network [35].

VPN client is connected to internet and then signals checked through firewall and only authorized signals will be passed to OEM computer. Virtual machines are connected to machines through SINEMA client server and SCALANCE S615.[35]

Industrial routers SCALANCE M

Remote machinery and factories can be connected to public or private networks using SCALANCE M industrial routers. Wireless communication is provided via GSM (2G), UMTS (3G), or LTE (4G), while wired communication is provided by ADSL, SHDSL, or PROFIBUS / MPI. The industrial routers are simple to incorporate into SINEMA Remote Connect, a remote network management platform that allows for simple and secure remote access to facilities and machinery.[36]

Security communication processors

Security communications processors defend against data tampering and espionage with its integrated firewall – which monitors data flow – and VPN. When setup through the TIA Portal, the security communications processors for SIMATIC controllers have the added benefit of automatically generating firewall rules. The firewall accepts configured communications connections automatically, which cuts down on configuration time and decreases the possibility of error.[37]

There are different software products used such as SINEMA remote connect for managing remote networks, SINEC NMS for network management and SINEC INS for network infrastructure services. Data is collected directly at the process, pre-processed, and made available towards other systems using SCALANCE LPE which is used for predictive maintenance, fault detection.[34]

3.3.3 Industrial wireless communication

In the industries, wireless communication brings up a lot of opportunities for effective automation systems. Siemens provides various industrial wireless solutions through WirelessHART, industrial wireless LAN to WiMAX. These solutions are used in different industries such as logistics, automotive.[19]

a) Industrial Wireless LAN

In control cabinet, SCALANCE W720 Client modules and SCALANCE W760 Access Points are used in machines for wireless networks with less cost. SIMATIC architecture benefits in less requirement of space while integrating components in IWLAN by standard IEEE 802.11n with 150 Mbps data rate.[38]

IWLAN in logistics

In logistics there is requirement of safe and low maintenance systems which should work efficiently. Shuttle system and retrieval systems are operated by IWLAN. The advantages of IWLAN are shown in figure.[39]

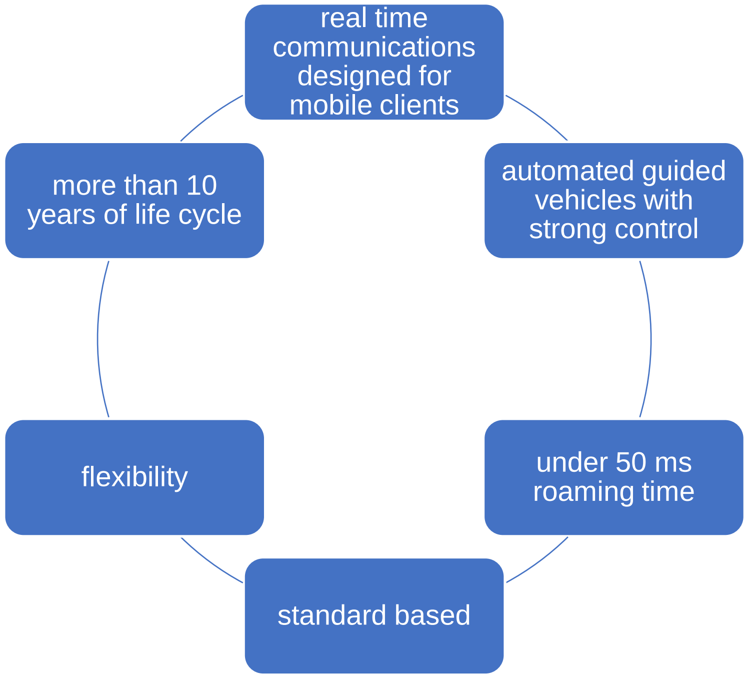

real time communications designed for mobile clients
automated guided vehicles with strong control
under 50 ms roaming time
standard based
flexibility
more than 10 years of life cycle

Figure 17: Advantages of IWLAN in logistics [39].

Example of IWLAN

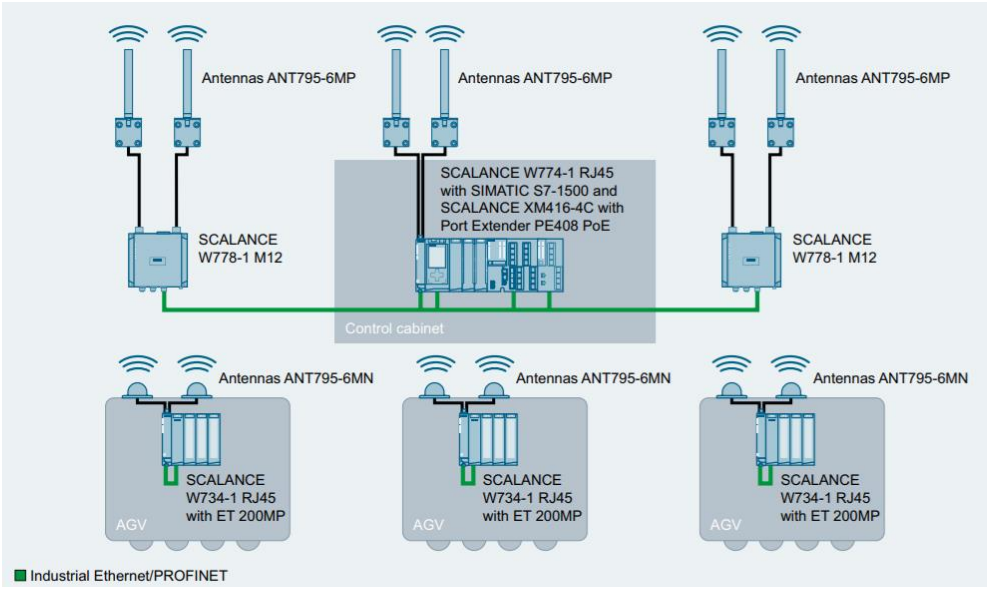

Antennas ANT795-6MP
Antennas ANT795-6MP
Antennas ANT795-6MP
SCALANCE W778-1 M12
SCALANCE W774-1 RJ45 with SIMATIC S7-1500 and SCALANCE XM416-4C with Port Extender PE408 PoE
SCALANCE W778-1 M12
Control cabinet
Antennas ANT795-6MN
Antennas ANT795-6MN
Antennas ANT795-6MN
SCALANCE W734-1 RJ45 with ET 200MP
SCALANCE W734-1 RJ45 with ET 200MP
SCALANCE W734-1 RJ45 with ET 200MP
AGV
AGV
AGV
🟩 Industrial Ethernet/PROFINET

Figure 18: IWLAN in logistics [39].

iPCF-MC in logistic applications for wireless communication

I/O devices and controllers used in PROFINET and EtherNet or IP applications are not able to communicate with IEEE 802.11 WLAN due to no presence of deterministic. iPCF is an industrial point coordination function in which iFeature focused on guided application solutions. iPCF-MC is more focused on solutions for freely moving participants in the network. The iPCF-MC is well suited to applications involving mobile clients that move about the field and EtherNet, PROFIsafe, PROFINET are used to set up communication with controllers. Alternative Access Points are always scanned by the Client with the help of iPCF-MC iFeature. If transmission of data is not proper then Access Point is quickly changed.[39]

b) Industrial routers

SCALANCE M makes wired and wireless communication possible. Fixed and portable workstations are possible to connect with main control and monitoring system by use of SCALANCE M wireless routers through LTE (4G), UMTS (3G), GSM (2G). SHDSL, PROFIBUS, ADSL are all supported by wired routers for connectivity of remote plants and equipment. All these routers are beneficial for networks which are IP-based.[36]

c) WirelessHART

WirelessHART pressure transmitter (SITRANS P280) gives process data, variables, functions with the help of radio. There is in built battery which consume low electricity and this transmitter can be mounted on rotating or moving equipment. There are different pressure transmitters available from 1.6 bar to 320 bar.[40]

WirelessHART temperature transmitter (SITRANS TF280) measures temperature from -200 to 850 °C with high security.[41]

3.3.4 Industrial remote communication

Nowadays industries are operated worldwide. So, solutions for remote communication plays an important role in production or process companies. Telecontrol and teleservice are applications used in remote communication.[19]

a) Telecontrol

Industrial plants need monitoring in which cost, and security are considered. Telecontrol is part of TIA which has open architecture for automation. Telecontrol focus on public and private remote networks. It is used when real plant location and control section are at long distance. It consists of control centre, RTUs (remote terminal units) and remote networks. RTUs collect data and send it to control centre. Then information is again sent back to the RTUs. For communication between RTUs and control centre, the remote networks are used such as internet or mobile wireless networks. Telecontrol protocols such as DNP3 IEC 60870-5-104,

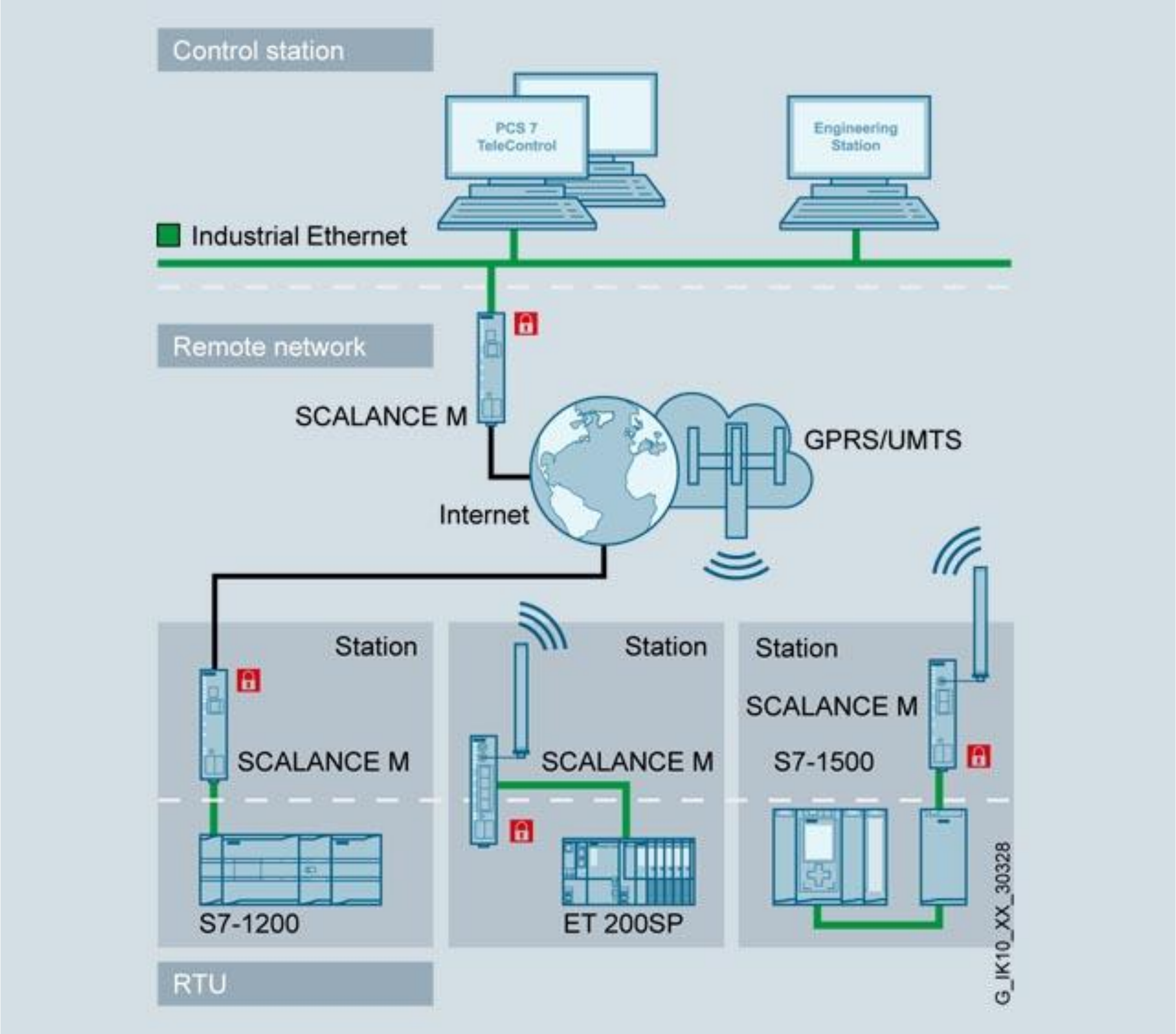


Figure 19: Setup of a telecontrol application [42].

SINAUT Telecontrol Basic are used to transfer data in mobile wireless networks. VPN tunnel is used to establish secure connection with the help of RTUs. Then data is transferred to the higher level for processing. There are different software solutions available for control centre such as TeleControl Server Basic is used for visualization via OPC UA. In complex applications, SCADA applications such as SIMATIC WinCC are helpful. Telecontrol systems such as IEC 60780, DNP3 and SINAUT S7 are possible to connect with non-Siemens systems via OPC. There are different accessories are available such as mobile network antennas, antenna connection system, cables, IP68 enclosure.[42]

b) Teleservice

The main use of Teleservice is remote maintenance and diagnostic like error detection, repair. It can send emails and text messages to reduce costs such as travelling costs or personal costs at workplace. SCALANCE M and SCALANCE S are used in Teleservice at plant and service station. The access to remote maintenance is established by SCALANCE M and access is wireless, also attacks are protected by VPN tunnel.[43]
The software used in teleservice is SINEMA Remote Connect. The connections can be made by DSL, cellular phone networks or private network. In different industries SINEMA Remote Connect is used such as OEMs, manufacturing, water, mechanical, plant construction.[44]

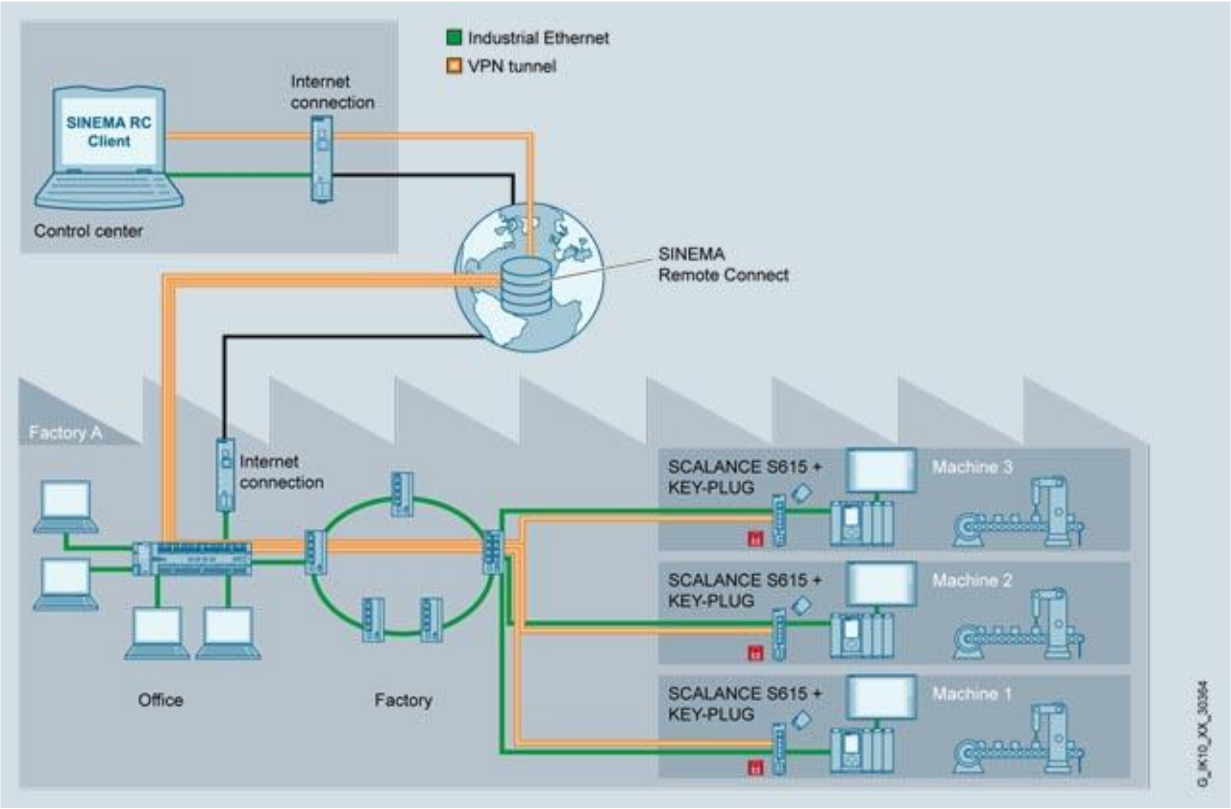


Figure 20: SINEMA RC configuration example: Remote service in series machine manufacturing [44].

SINEMA Remote Connect Server is operated from any location because it is available on PC with internet. All machines are connected with SCALANCE S615 by internal port and external port is used to connect SINEMA Remote Connect Server to VPN. SINEMA Remote client to server are connected with service centre with the help of PC. Operating systems used in SINEMA Remote Connect are Windows 10 pro, 2012, 2016, 2019 with 64 bits. In hardware SCALANCE S, PROFIBUS, communication processors, SIMATIC RTUs are needed to form whole system.[44]

c) Remote networks

Public and private networks are used in remote communication, and they have benefits like large bandwidths, less cost and high availability. The use of SCALANCE M is done in telecontrol, teleservice and remote applications. Integration of components is possible with TIA.[45]

The connection is possible with internet, mobile, telephone. The advantages are low operation expenses and investment for controlling, human expenditures and travel costs saved because of diagnostics, secured communication and SCALANCE products with five years of warranty. For example, Festo AG in Germany is using remote networks for expanding production area where integration of new machines needed few hours only instead of two weeks and plant has secure access. Another example, company in Oman called Mazoon Electricity Company where plant is located in dessert uses SCALANCE M, UMTS routers and antennas ANT794-4MR. This plant generates electricity and provides it to 1.5 million people. So, remote networks are usable in harsh environments.[46]

3.3.5 Rugged communications

The products used in rugged communication are known as RUGGEDCOM products which are

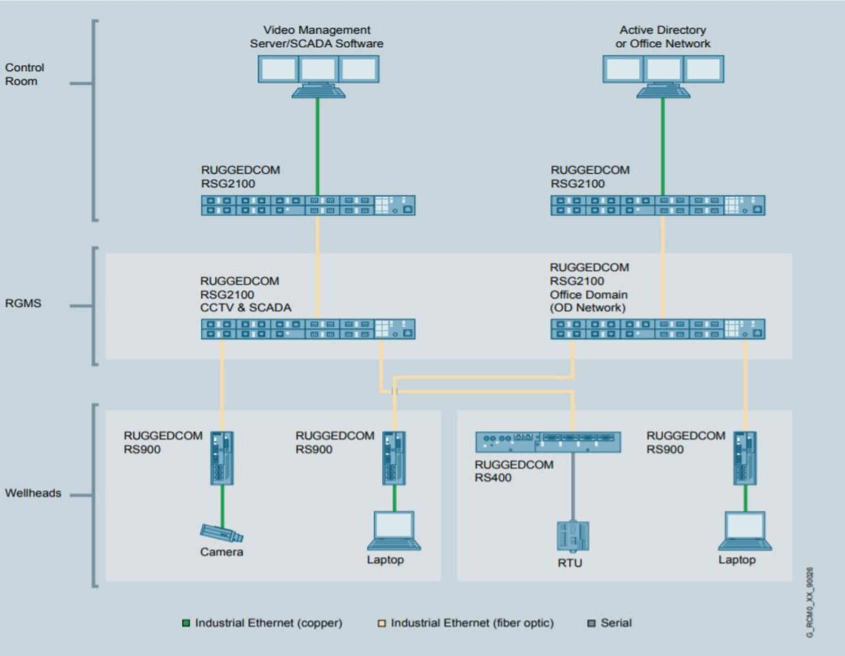

Control Room
Video Management Server/SCADA Software
Active Directory or Office Network
RUGGEDCOM RSG2100
RUGGEDCOM RSG2100
RGMS
RUGGEDCOM RSG2100 CCTV & SCADA
RUGGEDCOM RSG2100 Office Domain (OD Network)
Wellheads
RUGGEDCOM RS900
RUGGEDCOM RS900
RUGGEDCOM RS400
RUGGEDCOM RS900
Camera
Laptop
RTU
Laptop
Industrial Ethernet (copper)
Industrial Ethernet (fiber optic)
Serial
G_RCM0_XX_90026

Figure 21: Siemens solution for case study of PDO [47].

used in worst environments in industries such as transportation, electric plant, gas etc. Reliability and robustness are two key factors to establish standards. Zero packet loss technology is provided by these products.[48]

RUGGEDCOM RMS is media converter which is used in electric stations for converting two different medias [49]. RUGGEDCOM ethernet switches in layer 2 are used in challenging industrial situations and these switches satisfy standards of IEC 61850-3, NEMA TS 2, IEEE 1613 also compact and rack switches are available in layer 2 [50]. Layer 3 switches allow communication in two IP subnetworks [51].

The case study of Petroleum Development Oman (PDO) has oil and gas production plant and PDO wanted safe and reliable communication. Siemens provided solutions to work in such tough environment. RUGGEDCOM RS900 are available inside of wellheads for sending data. RUGGEDCOM RS400 serial servers in wellheads provides communication between RTU and SCADA. RUGGEDCOM RSG2100 installed at remote stations and local control room. Automated alarm is given in case of faulty actions by cameras. PDO saved cost and time due to Siemens network.[47]

3.3.6 Failsafe industrial communication

PROFINET allows simultaneous communication for standard IT communications and fieldbus communications. This single connection provides real time connectivity for the transfer of diagnostic data, process and user. For implementing PROFIsafe there no requirement of extra cabling. In conventional method huge number of wires are needed for safety relays. In comparison with technology of traditional wiring, fieldbus technology gives highly precise and detailed diagnostic information. The safe exchange of data with or without wire is possible in plants and machines by using PROFIsafe and PROFINET. The advantages of PROFIsafe and PROFINET are establishment of economical and efficient connections, less time required to transfer diagnostic information, possibility of wireless communication.[25]

ASIsafe is a bus used for high performance. ASIsafe provides safe, easy connections to actuators and sensors from field to upper level. ASI network provide direct connections with emergency switches. The advantages of ASIsafe are modular expansion, integration with PROFIsafe.[25]

In process industry, safety requirements should be according to standard IEC 61511. SIMATIC S7 safety matrix is a tool designed by considering standards. There is no requirement of programming languages, and safety logic is figured out easily from matrix of cause and effect.[52]

3.3.7 Industrial network solutions

The solutions make connection between operational technology and information technology efficient and reliable. Process starts with visit to site, and then current networks are studied.

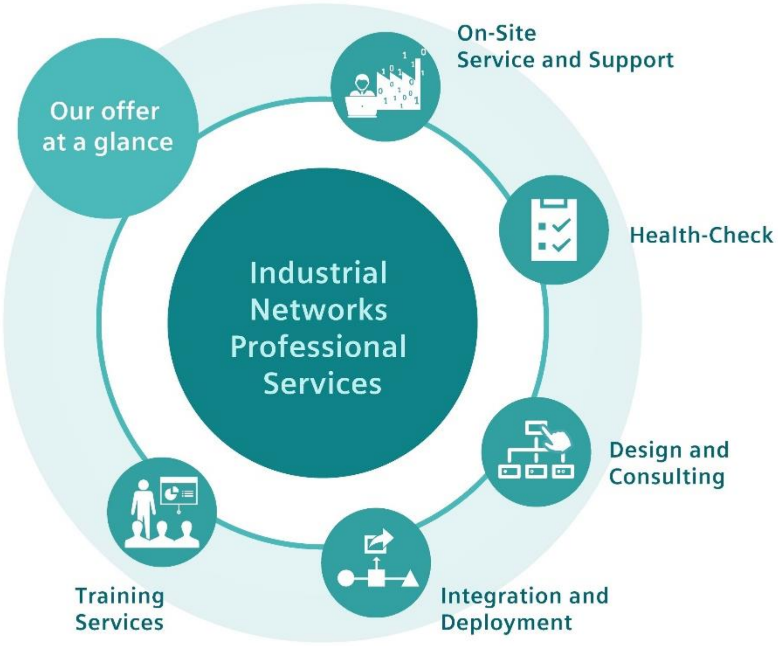

Our offer at a glance
On-Site Service and Support
Health-Check
Industrial Networks Professional Services
Design and Consulting
Integration and Deployment
Training Services

Figure 22: Siemens solutions from design to implementation [53]

Needs are identified to overcome deficiencies in current network for improving performance. Design of new network is done with consulting. Testing services reduce risks in failures and outages in networks. Implementation Services allow to benefit from speedy commissioning and assurance during the building stage, ensuring that plant and network run well. Training services are used to train plant employees for efficient working of plant.[53]

3.3.8 Network management

The SINEC is network management software that provides an overview of the whole network. It is used in the field of operational technology. It presents reports according to standards and problems are detected in the early stage. IEC 62443 is followed for security management. SINEC is divided into two software that are SINEC NMS and SINEC INS.[54]

Siemens NMS is known as network management system that is used to manage huge number of devices. SINEC NMS is designed according to FCAPS model in ISO. Northbound interface in FCAPS used to forward data to various systems such as HMI by OPC UA.[33]

Infrastructure network services is provided by SINEC INS for operational technology. It tells about time management, IP address management. It is easy to configure, quality service, saves time and scalable.[55]

4 Open Platform Communications – Unified Architecture (OPC-UA)

OPC is the standard used in automation for data transfer with security. The OPC foundation is in charge for developing this standard. The OPC standard is set of standards that specify connection between not only Clients and Servers but also Servers and Servers. It includes features like event tracking, real time, and historical data access. To overcome requirements like data modelling and secure connectivity in automation, OPC UA is developed.[56]

4.1 Introduction to OPC-UA

The OPC UA has architecture which is not only independent of platform but also service oriented. The specification goals are achieved by ensuring factors such as functional equivalence, platform independence, secure, extensible, and comprehensive information modelling architecture.[57]

Functional equivalence

The OPC Classic is only supported by Microsoft Windows and has achieved great success. But OPC UA and OPC classic are functionally equivalent, OPC UA can provide more than OPC Classic.[57]

Discovery	Search for OPC Servers running on PCs
Address space	Data structured in hierarchical manner, enabling OPC Clients to find and use simple and complicated structures
On demand	On allowed access, read, and write data
Subscriptions	Track data, provide violation notifications when changes happen depending on a client's specifications.
Events	Provide crucial information to clients according to their preferences
Methods	Clients are able to run applications according to methods given to the server

Table 2: Extra functions available in OPC UA [57].

Platform independence

Machine to enterprise, machine to machine and much more interconnections are offered by OPC UA. Hardware platforms such as cloud-based servers, PC hardware, PLCs, microcontrollers and operating systems such as Android, Microsoft Windows, Apple OSX, Linux are possible to use in OPC UA.[57]

Security

Firewall is not used in OPC UA, but security is controlled by other factors. The factors are defined in table. [57]

Transport	Ultra-fast OPC binary transport used for protocols
Session encryption	Safe transfer of messages by use of different encryption stages
Message signing	Allows recipient to authenticate origin and integrity of message
Sequenced packets	No chance of message reply attacks
authentication	X509 verify UA client and server
User control	Verified users are allowed
auditing	Tasks performed by users that are logged giving access audit trail

Table 3: Security factors [57].

Extensible

The different layer structure of architecture gives future proof platform. New technologies and existing systems both will be compatible in future.[57]

Information modelling and access

Information is gathered from data with the help of this framework. Access mechanisms such as execution of method, alerts for data and events, for current and old data the read and write actions, look-up mechanism to identify cases are introduced by OPC UA for information models. PubSub means publish-subscribe is another solution for event and data alerts.[57]

4.2 OPC UA specifications

There are different parts of OPC UA specifications.

4.2.1 Part 1: Overview and Concepts

The OPC 10000-1 UA specification is mentioned in part 1 as overview and concepts. OPC UA specification organization is divided into three parts and these parts are utility specification parts, access type specification parts, core specification parts. Main features of OPC UA are described from part 1 to part 7 as well as part 14 and all these features define layout of OPC *AddressSpace* and *Services*. OPC UA publish subscribe is defined in part 14. To describe access type, core capabilities are used. Part 12 discusses OPC UA discovery procedures, while Part 13 discusses data aggregation methods.[58]

Parts of core specification	**Parts of Access type specification**	**Parts of Utility specification**
Part 1 – Overview and concepts	Part 8 – Data access	Part 12 – Discovery
Part 2 – Security model	Part 9 – Alarms and conditions	Part 13 – Aggregates
Part 3 – Address space model	Part 10 – programs	
Part 4 – Services	Part 11 – Historical access	
Part 5 – Information model		
Part 6 – Service mappings		
Part 7 – Profiles		
Part 14 - PubSub		

Table 4: OPC UA Specification Organization [58].

According to [58], core specifications are defined below.

- OPC 10000-1 (part 1) specifications which describe the overview and concept about OPC UA.
- OPC 10000-2 (part 2) specifications that ensure secure connections in OPC UA.
- OPC 10000-3 (part 3) specifications which define layout and content of AddressSpace on the server.
- OPC 10000-4 (part 4) specifications describe the services that servers perform.
- OPC 10000-5 (part 5) specifications specify the types of servers and their connections.
- OPC 10000-6 (part 6) specifications describe mappings for transportation of protocol and data encoding.
- OPC 10000-7 (part 7) specifications specify the profiles which are present for applications in OPC UA.

According to [58], access type specifications are given below.

- OPC 10000-8 (part 8) specify OPC UA use in data access.
- OPC 10000-9 (part 9) specify access to alarms and conditions are supported by OPC UA.

- OPC 10000-10 (part 10) specify access to programs supported by OPC UA.
- OPC 10000-11 (part 11) describe historical access by OPC UA.

According to [58], utility specifications are given below.

- OPC 10000-12 (part 12) explain about operating various instances by Discovery server and interaction between clients and servers with Discovery servers.
- OPC 10000-13 (part 13) describe calculations of aggregates such as average, maximum etc.
- OPC 10000-14 (part 14) defines PubSub model for communication.

OPC UA is designed to focus on operations in higher level. For example, OPC UA interface can connect HMI to manufacturing execution systems. Further manufacturing execution systems can communicate with corporate enterprise through OPC UA.[58]

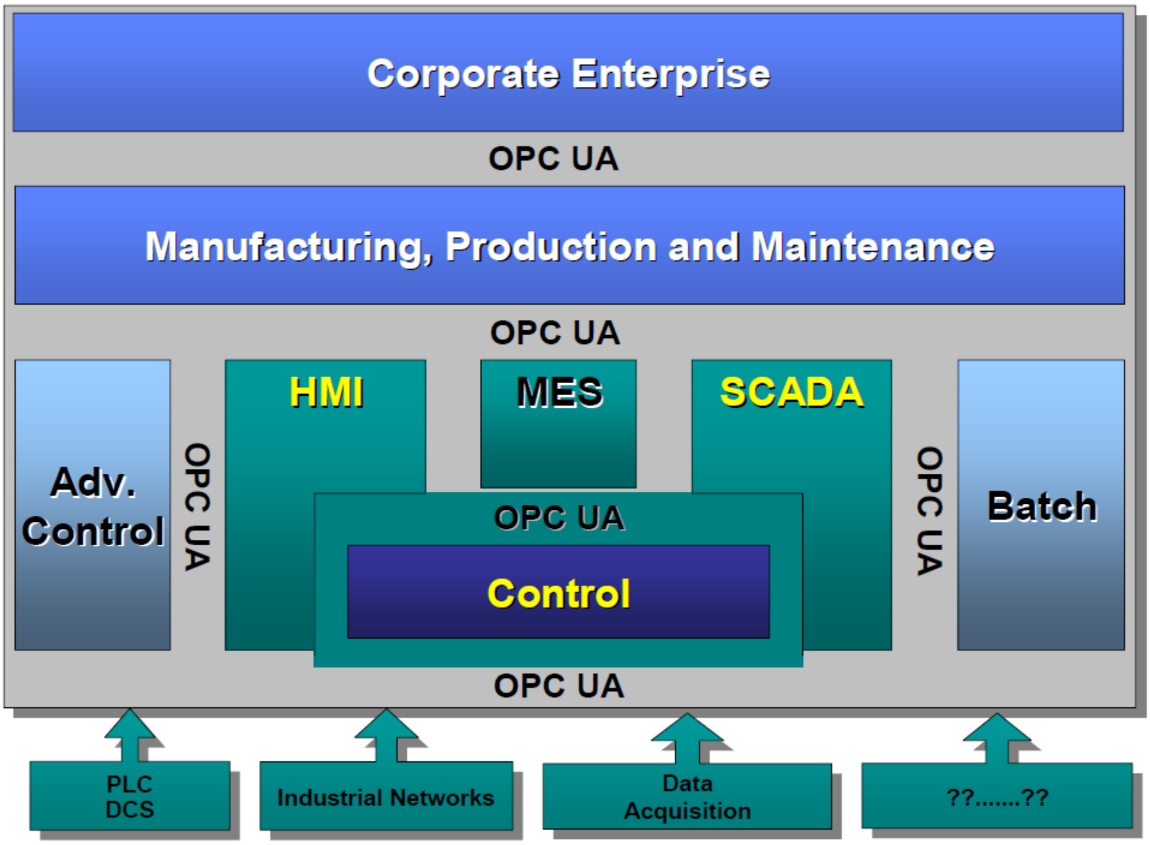


Figure 23: OPC UA target applications [58].

OPC COM servers are able to be mapped with OPC UA. JSON, UA Binary and XML/text are data encodings used in OPC UA also protocols such as HTTPS, OPC UA TCP, WebSockets are defined.[58]

4.2.2 System concepts

a) Client server overview

System architecture consists of *Servers* and *Clients*. There can be more than one *Server* and *Clients* in one system. One or multiple *Servers* can communicate with one *Client* and one *Server* can handle multiple Clients.[58]

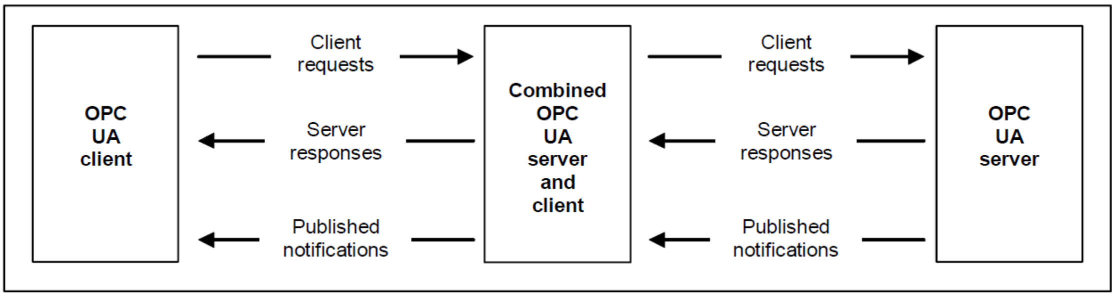


Figure 24: OPC UA system architecture [58].

b) OPC UA Clients

The programming that executes activity of client is known as *Client* Application. The *Client* API is used to separate OPC UA Communication Stack and *Client* Application. *Client* API calls are

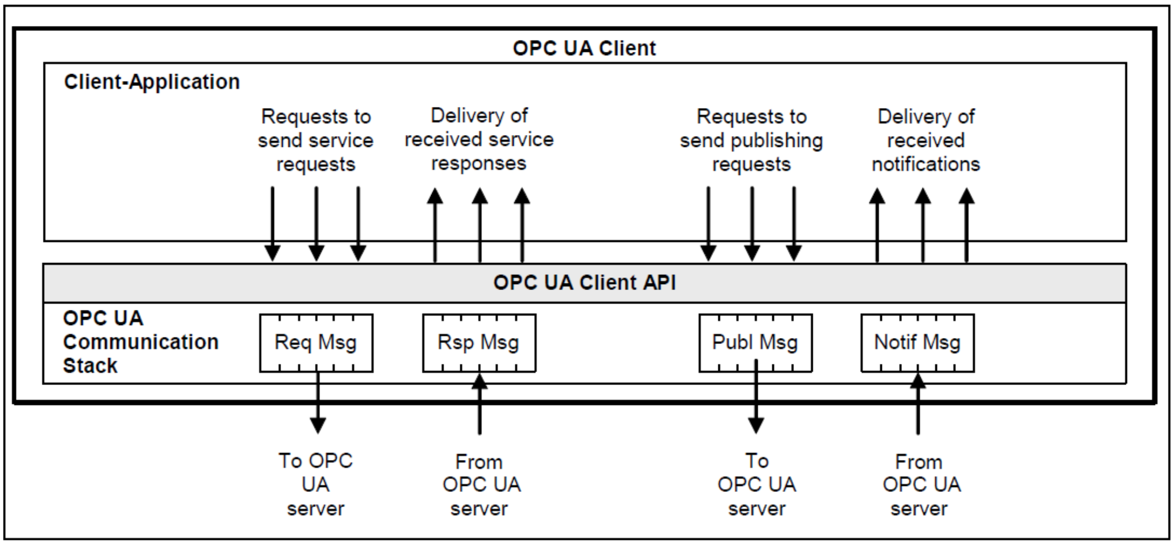

OPC UA Client
Client-Application
Requests to send service requests
Delivery of received service responses
Requests to send publishing requests
Delivery of received notifications
OPC UA Client API
OPC UA Communication Stack
Req Msg
Rsp Msg
Publ Msg
Notif Msg
To OPC UA server
From OPC UA server
To OPC UA server
From OPC UA server

Figure 25: OPC UA Client architecture [58].

converted into messages by OPC UA Communication Stack which also send these messages to OPC UA server. Responses and notifications are received by OPC UA communication stack and delivered via OPC UA client API to client application.[58]

c) OPC UA Servers

In the figure, main parts of server are shown with relation to each other. *Server* application accesses real objects such as software or hardware. *Server* Application is a program or code which is installed in *Server* for giving instructions to it. Messages from OPC UA *Clients* are send and received through *Server* API. Combination of set of nodes gives *AdressSpace* which can be accessed by the *Clients*. *Nodes* show real objects. *AddressSpace* has subset which is known as *View*. Total *AddressSpace* is *View* as default setting. *Clients* not only creates *MonitoredItems* but also monitor *AddressSpace Nodes*.[58]

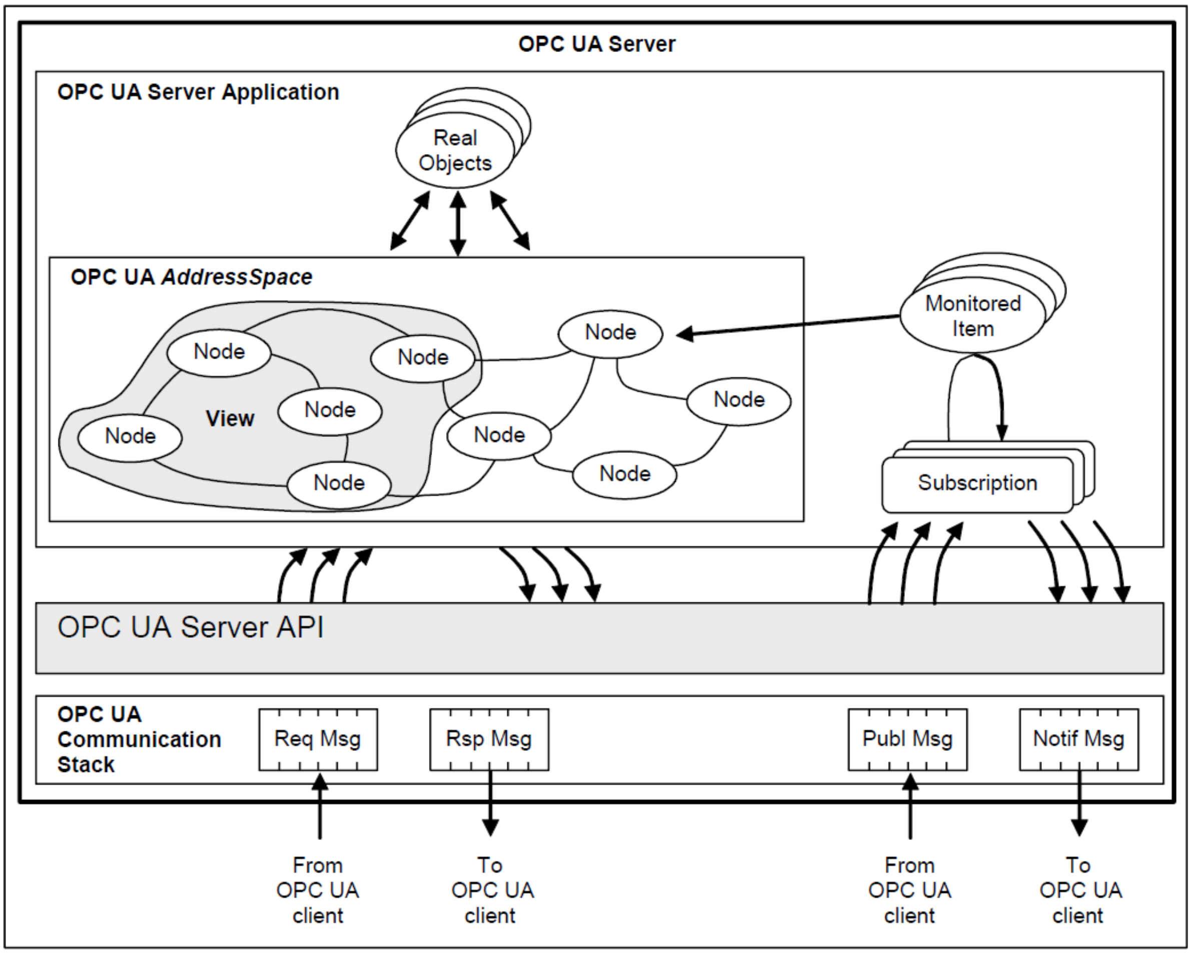


Figure 26: OPC UA Server [58].

OPC 10000-4 is used for OPC UA *Services*. *Clients* use request/response *Services* with the help of OPC UA *Service* Interface. Notifications are sent to *Clients* through *Publish Service*. Interactions between Servers are peer-to-peer or chained. OPC UA PubSub model is used to complete peer-to-peer interactions.[58]

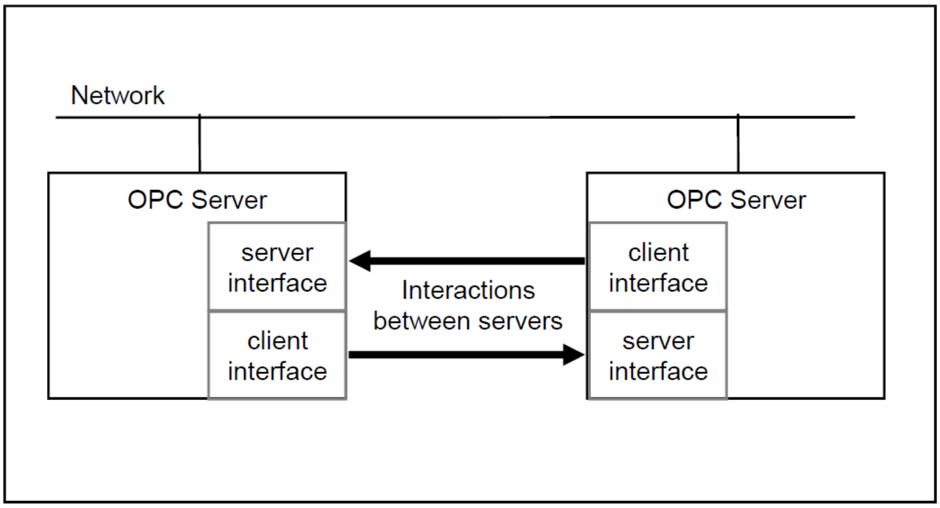


Figure 27: Peer-to-peer interactions [58].

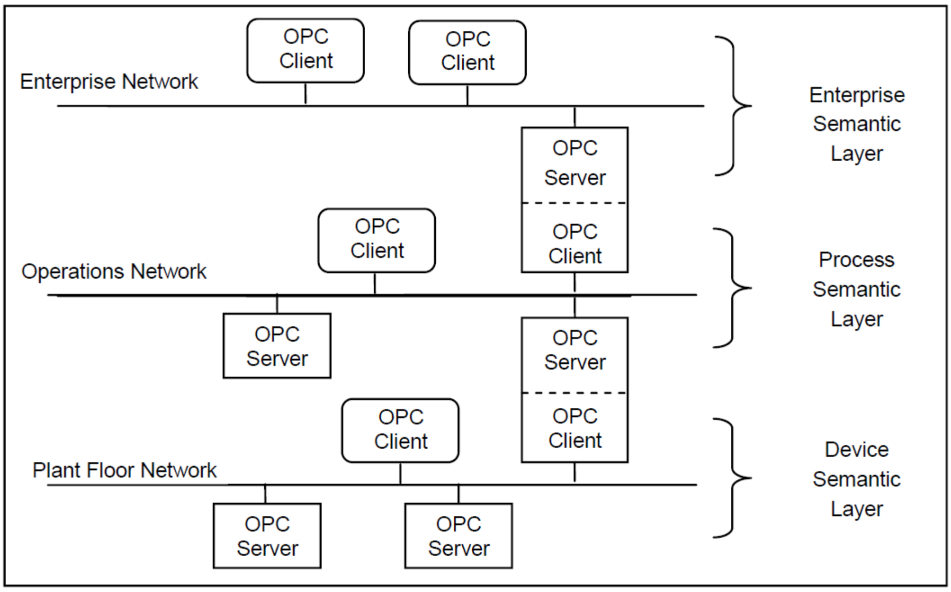


Figure 28: Chained interactions [58].

Chained interactions are used in company to connect vertical layers. Layers can be plant floor network, operations network, enterprise network.[58]

d) Redundancy

The main advantages of redundancy are fault tolerance, ensure system is always available, balance of load. Transparent and non-transparent are two types of *Redundancy*. All requirements are defined in OPC 10000-4.[58]

e) Publish-Subscribe

Message Oriented Middleware can be hardware or software which receive messages from *Publisher* without considering *Subscribers*. Requests and answers are not sent directly between OPC UA applications. *Subscribers* show curiosity in particular data without considering *Publishers.*[58]

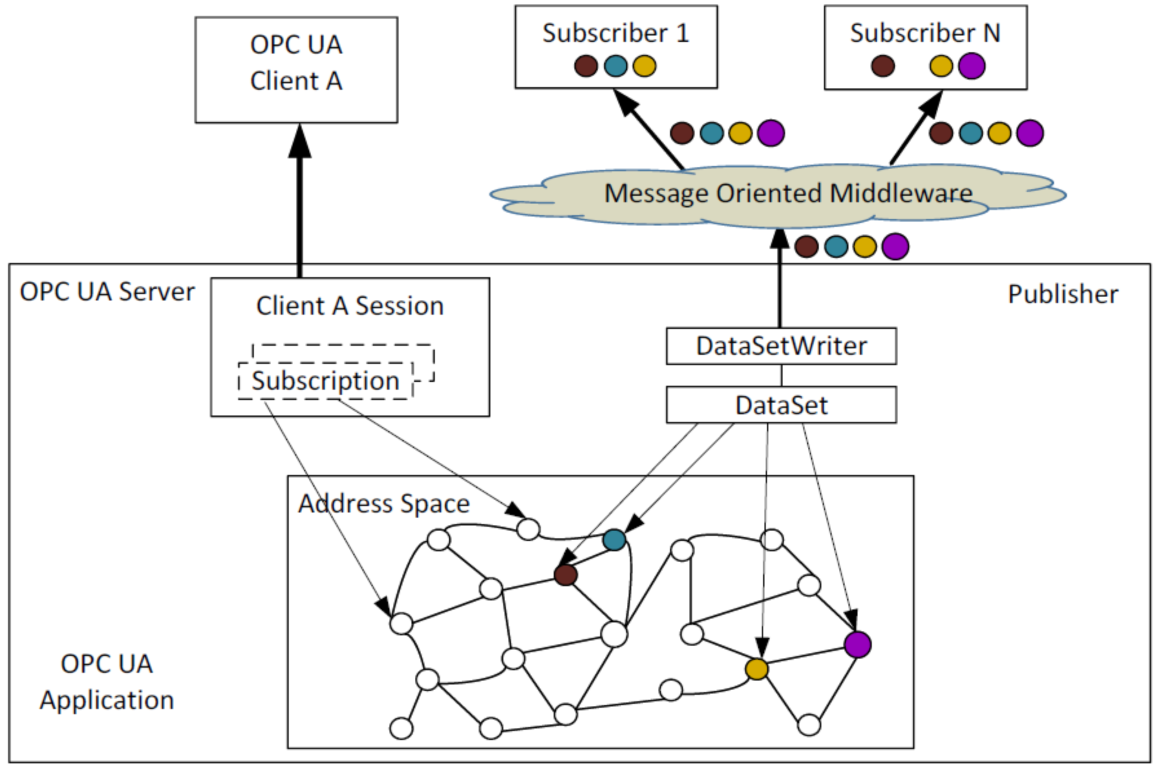


Figure 29: Integrated ClientServer and PubSub model [58].

OPC UA *PubSub* has two types of variants which are a broker-less form, broker-based form. In broker-less form, the network architecture that can route datagram-based communications is known as *Message Oriented Middleware*. In broker-based form, the broker is *Message Oriented*

Middleware and MQTT or AMQP protocols used to communicate *Broker*. *PubSub* is a messaging protocol that allows various system components to communicate without knowing one other's identities. The *Publisher* share data without any connection to *Subscriber.* There can be one or more than one *Subscribers,* but *Publisher* has no idea about them. OPC UA *PubSub* model is defined in OPC 10000-14. OPC UA *Information* model includes *Client Server* and *PubSub*. Mostly Subscriber is Client and Publisher is Server but other combination is also possible.[58]

4.2.3 Part 200: Industrial Automation Specifications

The standard covers modelling ideas for industrial automation. Specifications include statistical data and stacklights.[59]

4.2.3.1 Stacklight

A stacklight is audible or visual indicator of automation component’s condition or incident [59].

A) OPC UA ObjectTypes

BasicStacklightType

It is start point of stacklight which consist of various elements as shown in figure. *StacklightMode* tells about how stacklight unit is utilized. The ways in which stacklight is used are running light,

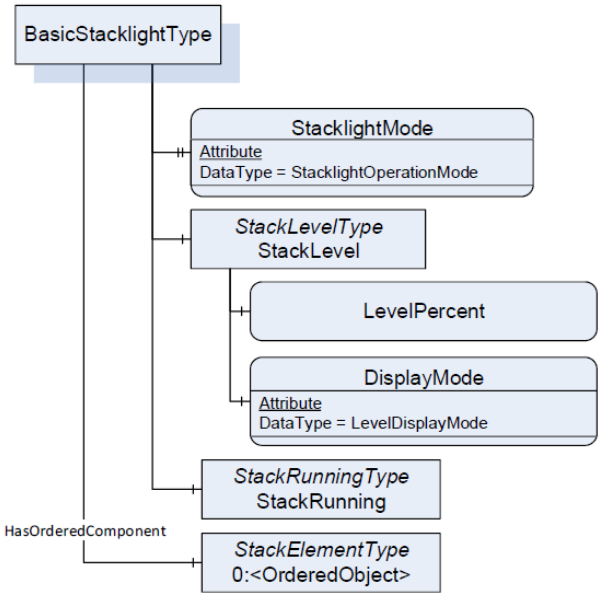


Figure 30: Overview of BasicStacklightType [59].

level meter. If stacklight is utilized in ‘Levelmeter’ then *stacklevel* is workable. If stacklight utilized as ‘Running Light’ then *StackRunning* is workable. 0:<OrderedObject> shows stack elements.[59]

Stacklighttype

It is used to get health condition of stacklight. In OPC 10000-100, *DeviceHealth* and *DeviceHealthAlarms* are defined. *DeviceHealth* gives information about health condition while

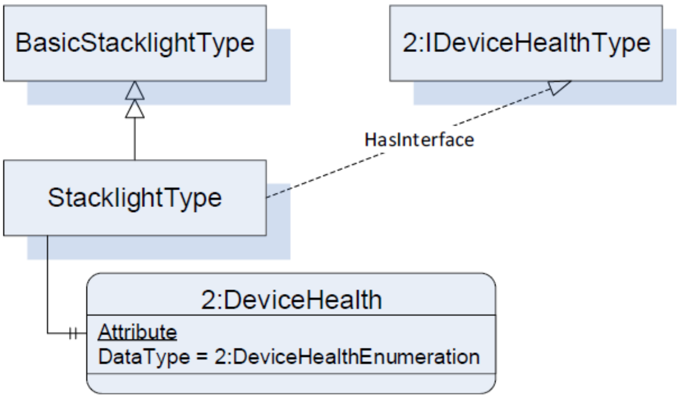


Figure 31: Overview of StacklightType [59].

DevivehealthAlarms talks about alarms of stacklight.[59]

StackLevelType

It gives information when stacklight is used as level meter. All values are in percentage.[59]

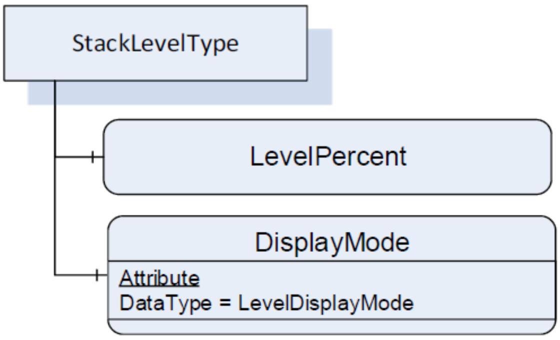


Figure 32: Overview of StackLevelType [59].

StackRunningType

It does not contain special information but shows stacklight as running [59].

StackElementType

It contains elements in stacklight which are in basic class. SignalOn is shown if signal is switched on or not by stack element. IsPartOfBase shows if in stacklight the element is contained by mounting base. 0:NumberInList count the stacklight elements in ascending order but starting at bottom.[59]

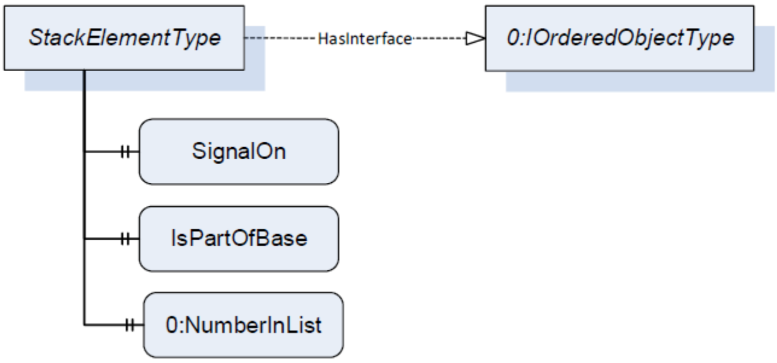


Figure 33: Overview of StackElementType [59].

StackElementLightType

It is used in stacklight to show lamp element. It consists of different parameters SignalColor, SignalMode, Intensity, <ControlChannel>. SignalColor is used to show colour after switching on the lamp element. SignalMode displays how the lamp is utilized such as continuous, blinking, flashing when the lamp is turned on. Intensity shown by brightness level varying from 0 to 100 percent. ControlChannel is used for control data of each colour element.[59]

StackElementAcousticType

Source paths involved are OperationMode, Intensity, AcousticSignals. OperationMode tells about which signal from AcousticSignalType nodes is used. Intensity is related to pressure level

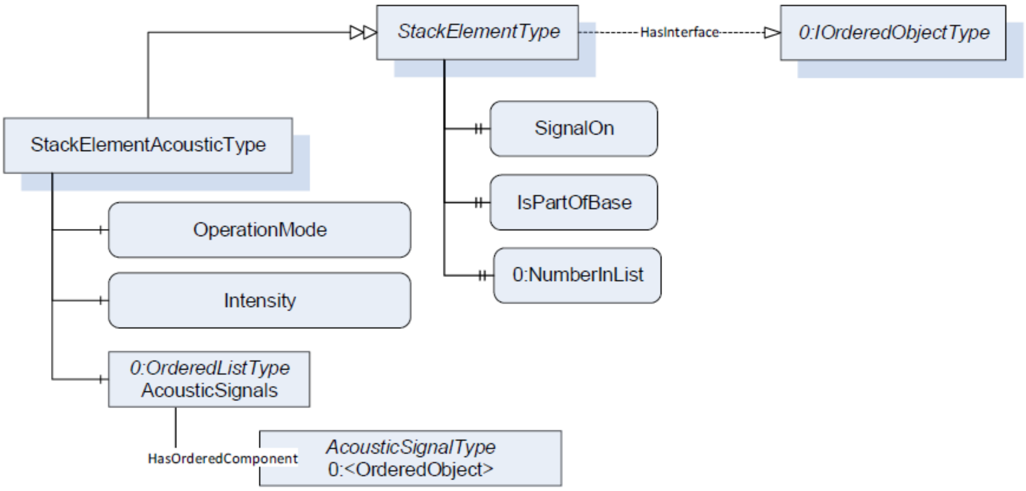


Figure 34: Overview of StackElementAcousticType [59].

of sound after switching on acoustic signal. List of the audio signals is given in AcousticSignals.[59]

ControlChannelType

It is defined by four factors which are SignalOn, ChannelColor, SignalMode, Intensity. SignalOn shows that colour is turned on. Colour of channel is shown by ChannelColor. Flashing, blinking

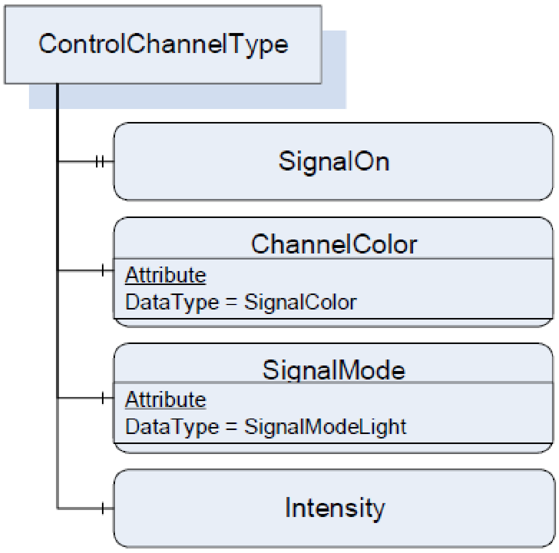


Figure 35: Overview of ControlChannelType [59].

and continuous are different modes for channel after turning on, included in SignalMode. Intensity means brightness of channel from 0 to 100 percent where 100 is highest.[59]

AcousticSignalType

It shows acoustic signal in ordered list. 0:NumberInList is used to count acoustic signals.

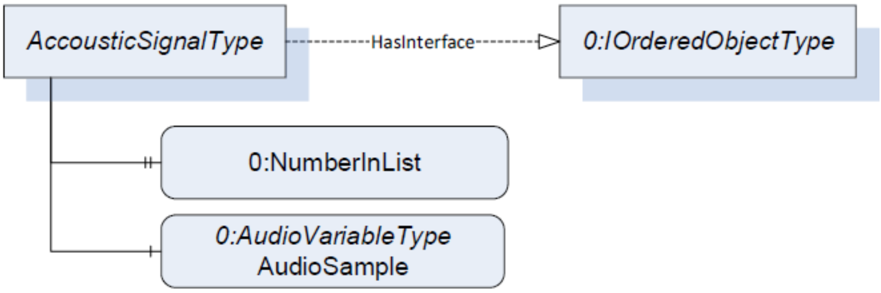


Figure 36: Overview of AcousticSignalType [59].

AudioSample includes audio data.[59]

B) OPC UA DataTypes

They are distributed into StacklightOperationMode, LevelDisplayMode, SignalColor and SignalModeLight [59].

StacklightOperationMode

It shows the values from 0 to 3 which tells about utilization of stacklight. Table mentions values and description.[59]

Name	Value	Description
Segmented	0	Stacklight refers to a collection of separate lights stacked together
Levelmeter	1	Stacklight as level meter
Running_Light	2	Whole stack used as running light
Other	3	How stacklight used is not defined

Table 5: Description of StacklightOperationMode [59].

LevelDisplayMode

This data type mentions values from 0 to 2 for showing percentual value when stacklight unit operates in mode of Levelmeter [59].

Name	Value	Description
Dimmed	0	Fractions shown by dimming
Blinking	1	Fractions shown by blinking
Other	2	Way not defined to show fractions

Table 6: Description of LevelDisplayMode [59].

SignalColor

In this data type, values from 0 to 7 are mentioned to show colours of stacklight lamps. Following table gives description of values.[59]

Name	Value	Description
Off	0	Disabled element
Red	1	Lamp colour is red
Green	2	Lamp colour is green
Blue	3	Lamp colour is blue
Yellow	4	Lamp colour is yellow (R+G)
Purple	5	Lamp colour is purple (R+B)
Cyan	6	Lamp colour is cyan (G+B)
White	7	Lamp colour is white (R+G+B)

Table 7: Description of SignalColor [59].

SignalModeLight

The settings in SignalModeLight are used to specify how a light responds when it is turned on. Values varies from 0 to 3 and following table explains what the values represents.[59]

Name	Value	Description
Continuous	0	Light is continuous
Blinking	1	Light is blinking
Flashing	2	Light is flashing
Other	3	Way is not defined for light

Table 8: Description of SignaModeLight [59].

4.2.3.2 Statistical Data

The framework for management of statistical data is provided [59].

IStatisticsType

The standard interface allows user to manage statistical data and get relevant data about them.

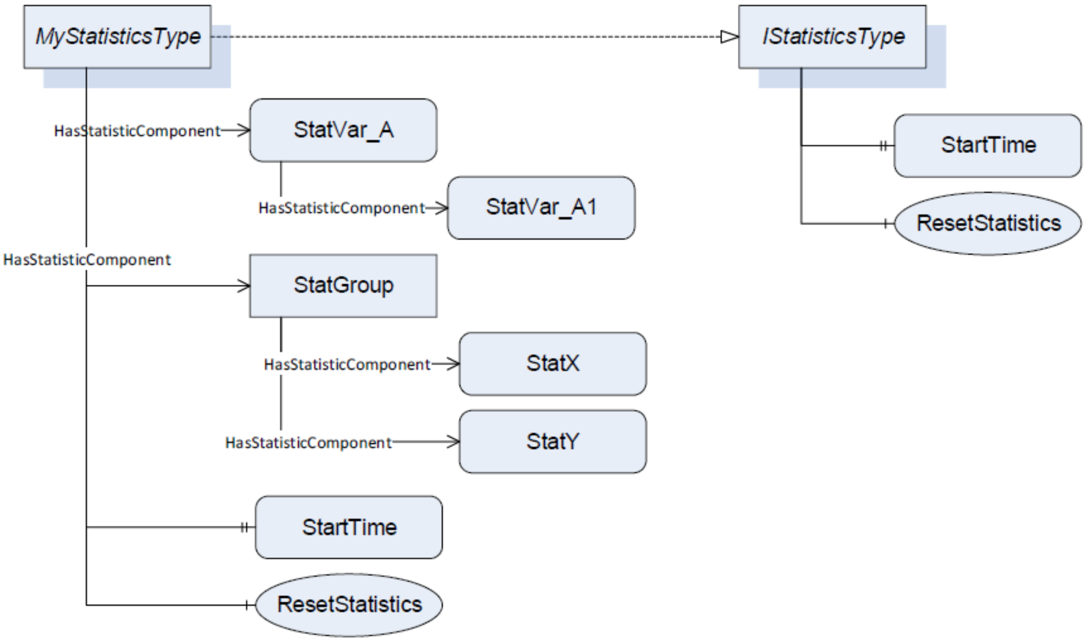


Figure 37: Use case of IStatisticsType interface [59]

The concrete statistical data is maintained in DataVariables that are either explicitly or implicitly accessed from the Object or ObjectType that implements the Interface with a HasStatisticComponent Reference. Those Variables are added by the concrete Objects or ObjectTypes that implement the Interface, not by the Interface itself. An example is shown in Figure. MyStatisticsType implements IStatisticsType and offers StatVar A and its sub-variable StatVar A1, as well as StatX and StatY, which are grouped by the Object StatGroup. The property StartTime, as well as the method ResetStatistics, apply to all of them. The StartTime indicates when all statistical data given by the Object implementing the Interface began to be gathered. The StartTime varies when the statistical data collection is reset. The subtypes of IStatisticsType are used for aggregating or rolling of statistical data. ResetStatistics is used for restarting of all statistical data.[59]

ResetStatistics Method

This method is used to reset all statistical data and here StartTime is current time. There are no Input or OutputArguments involved. The signature is given below.[59]

```
ResetStatistics (
);
```

IAggregateStatisticsType

It is subtype of IStatisticType Interface. From the beginning of the statistical data tracking until the tracking is reset, all data is considered. ResetCondition provides the cause and context for resetting statistics without using an OPC UA Client trigger, such as invoking the ResetStatistics Method. ResetCondition is a human-readable string that is vendor-specific. ResetCondition is a non-localized variable that may contain an expression that can be parsed by some clients. "AFTER 4 HOURS," "AFTER 1000 ITEMS," and "OPERATOR" are other examples.[59]

IRollingStatisticsType

It is another subtype from IStatisticType Interface. Not total data is taken into account for statistical data. WindowDuration is the duration in which data collection is done for statistical data.[59]

4.3 Industry 4.0 requirements and OPC UA solutions

Industry 4.0 has specific requirements to develop communication and digitalization. These requirements are satisfied by OPC UA. Requirements in Industry 4.0 and solutions by OPC UA are mentioned below.[60]

A) Independent communication

In Industry 4.0, there is requirement of independent communication. The communication should not be dependent on programming languages, manufacturers, industry, operating systems.[60]

OPC-UA solution

In technical point of view, OPC is not related to any particular industry. OPC UA is compatible with multiple system applications. The execution of even chip layer do not require operating system. It is not necessary to be a member to use OPC UA services or to create products of OPC UA. The OPC is not belonging to vendors and not making profit. OPC UA is universal protocol that is possible to use in any language. Nowadays the stacks in Ansi C/C++, Java and .NET are ready for use.[60]

B) Scalability

Scalability is important for connecting various platforms. The integrated networks are used for PLC controllers, cell phones, sensors, data centres, cloud platforms, PCs. The levels have vertical and horizontal connections.[60]

OPC UA solution

OPC-UA upholds an expansive scope of CPU structures and scales from a 15 kB impression (Fraunhofer Lemgo) to single-and multi-centre frameworks (Intel, ARM, PPC, and so forth). OPC-UA is utilized in implanted field gadgets such RFID scan, convention converters, and MES/ERP frameworks, just as practically all regulators and SCADA/HMI items. In the Amazon and Microsoft Azure mists, projects have recently been finished effectively.[60]

C) Security of data transfer

The data transfer between application and user level should be done securely with verification [60].

OPC UA solution

For verification of application, OPC UA applies user / password, Kerberos or X.509 certificate. The stack supports authenticated and protected data transfers. The auditing feature are supported by stack.[60]

D) Service Oriented Architecture

Service oriented architecture (SOA) and transport are required in Industry 4.0 for various operations. The standards used for swapping of past and current data, events and commands are TCP/IP (transmission control protocol and internet protocol).[60]

OPC UA solution

Transport method has no influence on OPC UA. The two interfaces used at moment are TCP and HTTP/HTTPS. The systems with high performance use an optimized TCP-based binary protocol. The web applications with XML or binary coded message use HTTP/HTTPS. The implementation of PubSub mechanism is possible. The stack ensure that all data is sent in a consistent manner. OPC UA standardizes historical data and its mathematical aggregation. The token-based mechanism is used for events and alarms.[60]

E) Mapping of information

The complex information content should be mapped to model virtual elements for showing real products and manufacturing processes.[60]

OPC UA solution

OPC UA gives completely networked idea for not only hierarchical but also full meshed network. The address space used in OPC UA is object oriented. Object structures may be created by referring instances and their types, as well as a type of model which is possible to expand with legacy. Servers convey case and framework type, customers able to explore via this organization and get the data they want, in any event, for types that were obscure to them previously. That is prerequisite for plug and produce capability that does not require the devices to be configured beforehand.[60]

F) Autonomous connections

Unplanned, the function of plug and produce uses ad hoc communication with the help of access data. The ad hoc mode permits direct communication among computers without use of router. The offered services for autonomous engagement in “smart” networked environments by combining components.[60]

OPC UA solution

To identify and notify OPC UA devices and their operations, various “discovery” procedures are characterized by OPC UA. Members in OPC UA can be found in subnet, worldwide or local. Network contestants are addressed and identified using subnet aggregation and intelligent configuration less procedures.[60]

G) Integration in semantic extension and engineering

The industry 4.0 able to get integrated into field of engineering and the semantic extension [60].

OPC UA solution

The OPC foundation as of now works together effectively with different associations such as AIM, PLCopen, FDI, BACnet. It is at present growing its collaboration for example ISA95, MDIS, MES-DACH. AutomationML has launched a new collaboration project with the goal of improving interoperability amongst engineering tools.[60]

H) Similarity confirmation of standards

The confirmation of similarity should compliance with defined standards [60].

OPC UA solution

The OPC UA is as of now an IEC 62541 standard. For testing and guaranteeing similarity the instruments and test research facilities are accessible. For corrections and extensions, the extended tests are needed. Furthermore, different approvals are with respect to information security and functional safety are carried out by certification bodies and external test.[60]

5 Use cases OPC-UA and solutions in Siemens

In this chapter, OPC UA use cases are explained and solutions are provided by Siemens.

5.1 OPC-UA and PROFINET

In Siemens, the vertical axis is divided into two parts in which one part is PROFINET and second is OPC UA. At field level PROFINET is used and from control level OPC UA is used in TIA. OPC UA ensure vertical connectivity to cloud and M2M communication. OPC UA is ideal companion to PROFINET. These standards help for communication with no troubles in digitalization. Advantages of both standards are possible to use in one system. At the field level, PROFINET excels with deterministic, a wide bandwidth for growing signal counts, and rigorous real-time capabilities for ever-faster applications. OPC UA connects machine to machine, machine to manufacturing execution system, machine to cloud (MindSphere).[61]

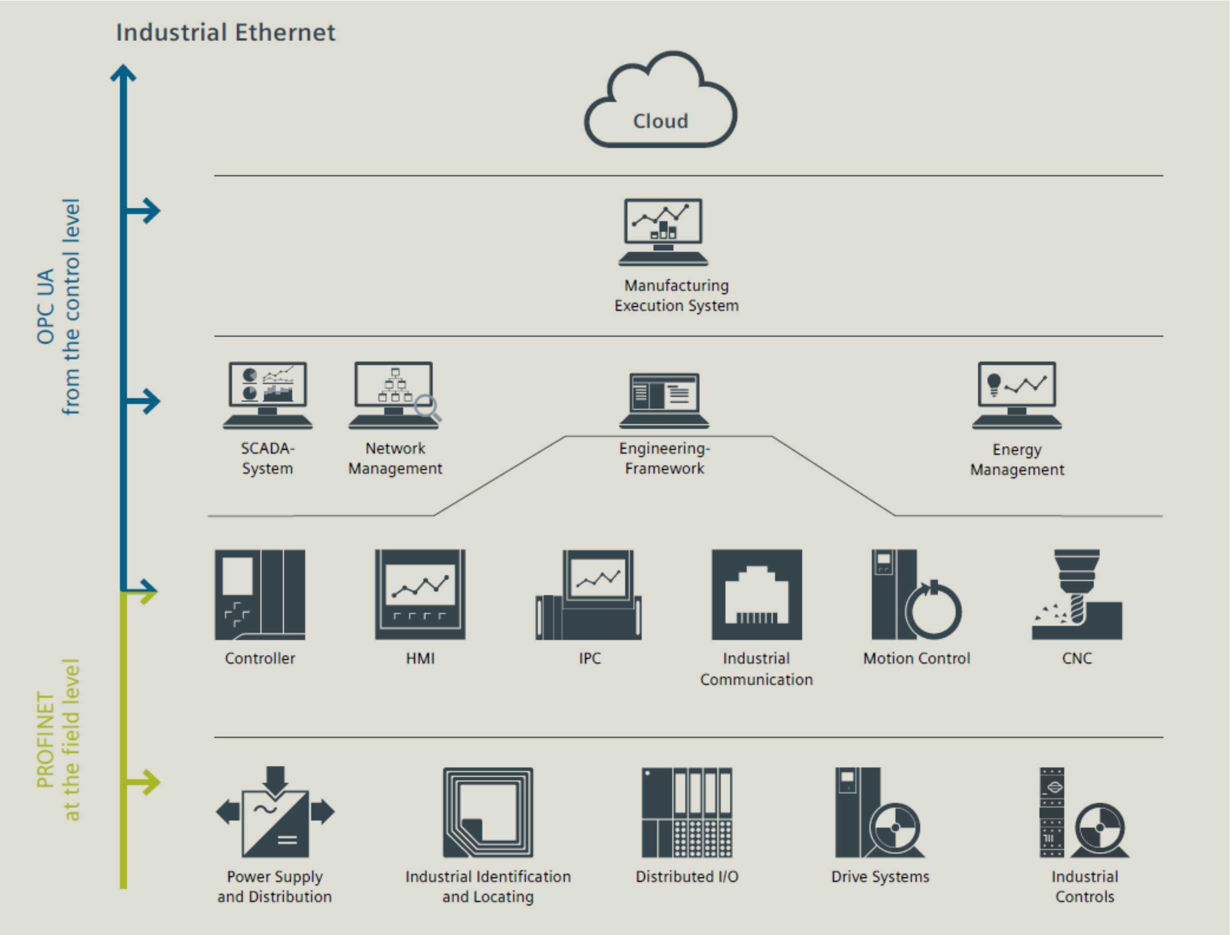


Figure 38: Siemens OPC UA with PROFINET [61].

OPC UA has openness means it is not influenced by platform and vendor which help to build required configuration. There is possibility of direct integration of OPC UA in HMI, controllers etc. OPC UA can operate parallelly with PROFINET up to countless number of actions. It is scalable for extension of plants. According to requirement, communication can be set such as PubSub or client/server.[61]

PROFINET standard is used at field level because it is flexible, efficient. It has no influence of vendors. IEEE conformity plays important role in future progress. It is easy to approach anywhere due to web-based tools. It provides ring, star, tree, line networks which make flexible. It is an open standard to provide communication for automation devices and standard ethernet. PROFIsafe is used for protection of machines, humans, and environment.[61]

OPC UA simple ethernet based networking and has capacity to exchange complicated information models. Industrial ethernet can be simply integrated with PROFINET. OPC UA provides protection by encryption and authentication. No requirement of extra hardware for security of communications because there are direct protocols for security.[61]

PROFINET reduces wiring cost because a single wire connects IT network and machines. It's simple to change out devices since the I/O controller will detect and "baptize" the new one. FastConnect provides simple cabling. Inspection of networks and devices can be done from faraway areas via remote access. PROFIenergy ensures high energy efficiency by turning off consumers who are no longer required. Huge systems can be formed because up to 1024 devices can be linked in network. Excellent data speed is possible due to high bandwidth. PROFINET detects and connects devices to I/O controller in less than 500 milliseconds. So, this proves quick start of system. PROFINET produces exceptionally precise cycles of 125 microseconds with uncertainty of 1 microsecond.[61]

Integration of OPC UA and PROFINET in industrial ethernet

OPC UA is open and has no influence of platform which assures easy connection with third party applications, and expansion is possible to achieve targets. OPC UA enables more than simply data transport thanks to its semantic capabilities, it also has its own information model. A secure connection is guaranteed by well-established security procedures such as authentication, authorisation, and encryption.[2]

Use case of protocols

The models are used for protocols such as PubSub, Client-Server. The use of these models is decided according to application. If there is requirement of scalability in application where huge quantity of data points is contacted for each modification, then PubSub protocol is used for communication. If there is requirement of specific result once in a while, then it is better to use Client-Server protocol for communication.[62]

Use case for OT-IT horizontal communication

By considering situation where controllers and sensors interact with each other. The deployment of OPC UA Pub-Sub is possible. Second use case is communication between PLC to PLC where OPC UA is implemented with deterministic IP communications.[62]

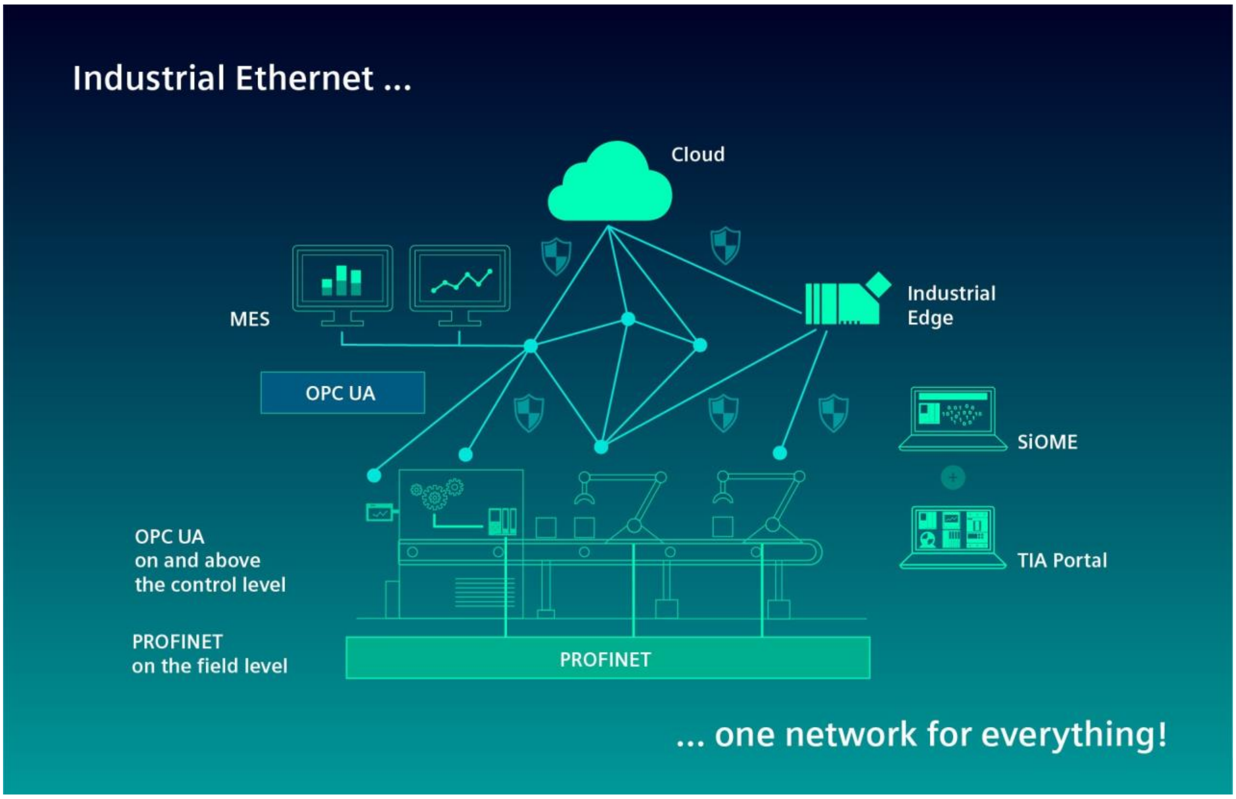

Industrial Ethernet ...
Cloud
MES
Industrial Edge
OPC UA
SiOME
TIA Portal
OPC UA on and above the control level
PROFINET on the field level
PROFINET
... one network for everything!

Figure 39: Integration of OPC UA and PROFINET in industrial ethernet [2].

Use case in IT level

OPC UA is possible to use in MES or predictive maintenance applications.[62]

Use cases of OPC UA in Siemens project

In this use case, S7-1500 is used as OPC UA server. The data is collected with the help of S7-1500 which provides services such as subscriptions, write, read etc. The clients are SIMIT V9.1 and OPC Scout V10. The SIMIT V9.1 is software for process simulation which can be used for testing of automation software, documentation of entire factory, simulating devices etc. The OPC Scout V10 compatible with OPC UA as well as used in showing alarms, controlling, checking of connection, browsing by using function “Discovery”, writing, and reading of values etc. OPC UA server data from Excel is obtained by OPC UA client library. The OPCLabs library is possible implement in Excel worksheet. This project uses OPC UA to gather data of SIMATIC S7-1500.

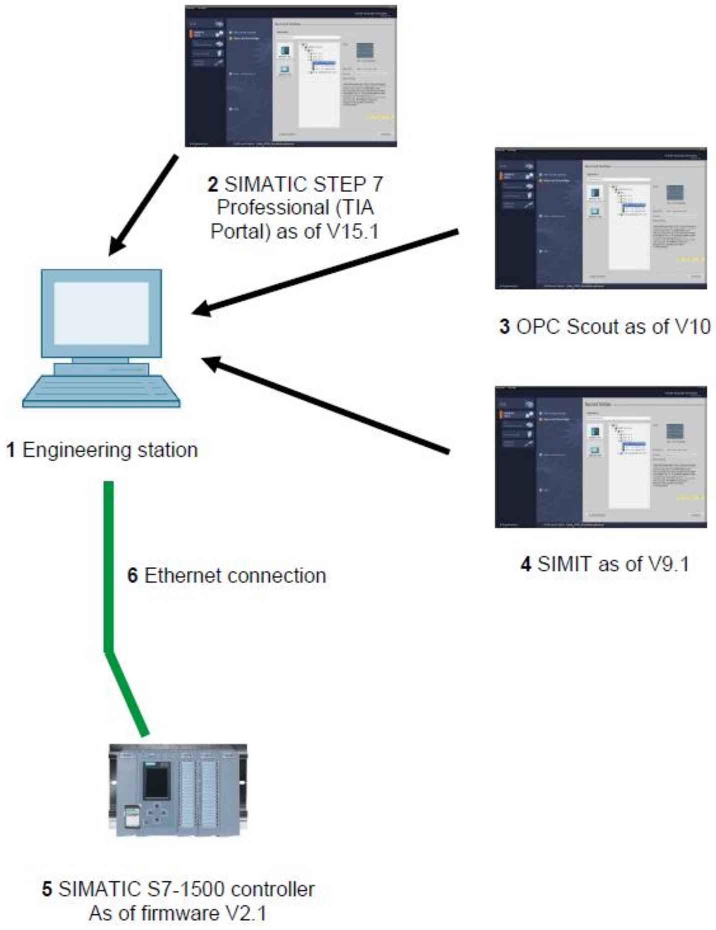

2 SIMATIC STEP 7 Professional (TIA Portal) as of V15.1
3 OPC Scout as of V10
1 Engineering station
4 SIMIT as of V9.1
6 Ethernet connection
5 SIMATIC S7-1500 controller As of firmware V2.1

Figure 40: Use of OPC UA in Siemens project [63].

The engineering station and SIMATIC S7-1500 are connected through ethernet connection.[63]

OPC UA in SIMATIC S7-1500

The use case of client for OPC UA data access is shown in figure. OPC UA client V15.1 is used in communication between machine to machine for exchange of data. The OPC UA client V15.1 also establish connection from machine to upper level such as SCADA, MES. The two servers are used to connect upper level to machine are OPC UA server S7-1500 V14 and OPC UA server S7-1200 V16.[64]

The OPC UA server is used for various functions mentioned in this paragraph. The data browsing is done by browsing function. OPC UA server get browse request from OPC UA client and then this request is processed by OPC UA server. The browse response is sent back to

OPC UA client by OPC UA server. The data access that is acyclic is provided by function read/write. The R/W request is sent to OPC UA server by OPC UA client. OPC UA server send R/W response to OPC UA client. The tremendous throughput with repetitive acyclic access is possible by utilizing registered read/write. The registration of nodes and R/W request are sent by OPC UA client to OPC UA server. The OPC UA server send node handles and R/W response back to OPC UA client. The subscription function is used to reduce work of applications such as

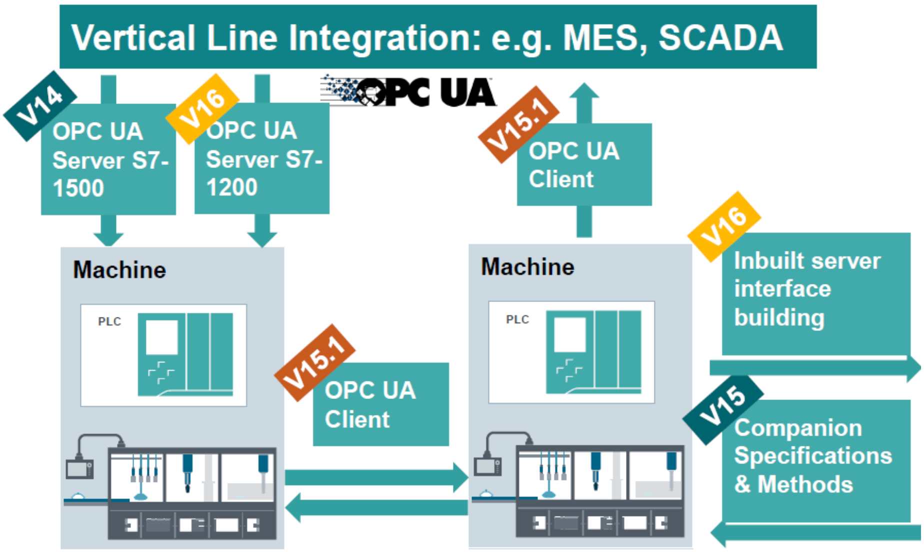


Figure 41: OPC UA data access client [64].

HMI. The sampling and publishing processes are used by OPC UA client and OPC UA server. The methods provide data exchange which is generally consistent. The OPC UA sent call request to OPC UA server and then call response is send back to OPC UA client. Information models are given by companion specifications.[64]

	S7-1500	S7-1200
Browsing	Yes	Yes
Read/Write	Yes	Yes
Registered Read/Write	Yes	No
Subscription	Yes	Yes
Methods	Yes	No
Companion specifications	Yes	Yes

Table 9: Usage of S7-1500 and S7-1200 [64].

The table shows functions that are performed by S7-1200 and S7-1500. The server has browsing function which helps in PLC data browsing. The PLC data which is presented in symbolic format is accessed by read function with the help of server. Also, the server has written access to PLC data in symbolic format. The registered read allows server to have repeated access to PLC data. In subscribe function, the publish request is sent to OPC UA server by OPC UA client. And after this the publishing is done via OPC UA server.[64]

Use case in access type of OPC UA and SIMATIC CPUs

Access type recommended	Use case
Read/Write	Data is accessed for few occasions or one time
Subscription	Data read in cyclic format, Data monitoring
Registered Read/Write	Data access to designated nodes with excellent performance
Methods	Data transport is consistent, Handshake is not required

Table 10: Recommended access types for use cases [64].

OPC UA use case in quantity structures

If there are no time restrictions in small quantity structures, then data from controller can be directly sent to cloud via cloud gateway. The communication between cloud gateway and controller is set via OPC UA. The example for this use case is send energy data and status of machinery to gateway of cloud. The number of data points used per second are 100.[64]

In large quantity structures the integration of different devices is needed. The MES, HMI, SCADA are used with OPC UA standard. Here quantity of data points is 1000 per second.[64]

Use case of monitoring via HMI

Subscriptions must be defined in accordance with the displaying methods because it is important to prevent unwanted communications. The parameters which seem to be visible must be enabled. At the time of connection establishment, the subscriptions must be generated. While execution, the subscriptions must be rarely updated to avoid log-on procedure load. Various update cycles must be used for data where one cycle shows single, or many devices are monitored with subscription. For example, data cycle can be 1s, 5s.[64]

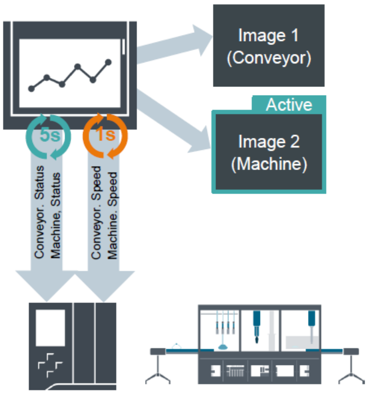


Figure 42: Monitoring with HMI [64].

Use case of OPC UA with upper-level systems

In case, MES receives request from machinery. The exchange of data is started from PLC. The controller is OPC UA client in this situation. If operator updates a value in SCADA system, then data exchange is started from SCADA to controller. So, controller is used as server.[64]

Practical use of OPC UA in third party SCADA

In particular situation, the design requirement is PLC and SCADA should be connected via OPC UA. Also, the single variables cross limit of 10000 monitored elements in quantity structure. The problem can be solved by dividing data into various publishing and sampling intervals such as 5s, 100ms, 1s. The prevention of unwanted communication is solved by deactivation of useless data point.[64]

5.2 OPC UA in TIA Portal

The automation services are digitalized through Totally Integrated Automation (TIA) Portal. The advantages of TIA Portal are enhanced plant productivity with the help of efficient management of energy and extra inspection of plant. TIA Portal provides transparency in processes. The simulation tools are used to reduce time to market. [65]

5.2.1 TIA Portal

In digital enterprise the automation and digitalization can be achieved through TIA Portal. The TIA Portal has digital workflow which helps in evaluating and testing of each element in project without creating real things by using virtual design of plants and machines. To achieve high quality “digital twin” is linked with cloud and operational IT. Digital workflow contains simulation of HMI and controls with whole plant. So, there is reduction in commissioning time. Automation simulation is flexible because of PLC modules can be checked fast, modelling of plant is done with SIMATIC S7-PLCSIM Advanced by considering switching and time sequences, designing of model is completed by SIMATIC STEP 7, high level languages (C, C# etc.) used to design models with high degree of complicacy with PLCSIM Advanced interface. Software generators are used to construct projects quickly then redundant operations are decreased. Teamcenter can combine various project versions worldwide. Workflows are available at any time and at any place by using cloud solutions (TIA Portal Cloud connector).[65]

Integrated engineering helps to decrease time required for engineering. Integration of main elements in project is done by TIA Portal. Numerous individuals able to work on a project simultaneously by using TIA Portal Multiuser Engineering. So, working on projects is highly flexible. Encourage the adoption of business standards by way of a simple definition management of TIA Portal libraries' program code. The factors such as code templates with extensive programming, variety of new and improved testing equipment, while commissioning live recordings are taken to analyse random effects save extra efforts and time required to positively diagnose and promptly rectify issues. SIMATIC Visualization Architect is able to produce HMI visualizations. Due to comprehensive library storage reuse of different objects is possible which protect from duplicated work. As international rivalry heats up, it's more important than ever to understand what's going on within a machinery. Because of continuous data and detailed statistics, clear operation helps to achieve the correct judgments. It further improves energy efficiency, which also is becoming an increasingly significant aspect in enhancing ability to compete.[65]

5.2.2 TIA Portal software

The integration of software such as WinCC, STEP 7 etc. is possible with TIA Portal. The advantages such as energy management by using SIMATIC Energy. In industry 4.0 criteria there is need of digital organization which is satisfied by TIA Portal.[66]

Software **Function**	**STEP 7**	**WinCC**	**Startdrive**	**Safety**
HMI visuals are produced automatically		✖		
Diagnostics for machines and plants	✖	✖		✖
From integrated collection of energy information to strategic load control	✖	✖		
Monitoring the style guide and running an automated application test	✖			✖

Engineering software control through cloud	✖	✖	✖	
TIA Portal for commissioning and team engineering	✖	✖		
TIA Portal for management of clients	✖	✖	✖	
Teamcenter for storing data centrally and cross-discipline	✖			
Engineering activities may be automated, and expanded functionality can be used in a variety of ways	✖	✖	✖	
Simulation and functionality testing for automation	✖			
MindSphere connection	✖	✖	✖	
Windows and real-time modules are being developed	✖			
Utilization of Matlab controller which is closed loop based on model and simulations of machinery	✖			
Portable as well as any device can supervise and operate		✖		
Control level and machines has communication standard	✖			
Analysis dependent on conditions and energy efficiency calculation	✖	✖		
Safety related functions in programming	✖			✖
In space, kinematic motions controlling	✖			✖
Production data storage for the long duration		✖		
Dashboards on the web for clear production data		✖		
User administration is centralized and plant-wide		✖		
Traceability of operator activities in accordance with GMP		✖		
Commissioning and coding of robots	✖	✖		
Technological advancements in the SINAMICS driving system are being programmed			✖	
Safety features of the SINAMICS drive system must be accepted and documented			✖	✖
Create cutting-edge HMI systems and operational philosophies		✖		

Synchronous, dispersed functioning of SCADA operator units located at different locations		✖		
Enhanced SCADA system presence as a result of redundant architectures		✖		
Logging of process values and alarms		✖		
Recipe development, application, and distribution		✖		
SIMATIC HMI systems may be controlled and monitored remotely by an operator		✖		
Control and monitoring of the operator are both done on the web at the same time		✖		
Data transfer between manufacturing and the IT sector is bidirectional		✖		

Table 11: TIA Portal software and functions [66].

The functions are used in operation of plant, integration of line, development of software, commissioning of machine, services of machinery. For example, in line integration there is requirement of diagnostics of plants and machinery which is included in software such as STEP /, WinCC, Safety. In line integration, the controlling and functioning which is not dependent on devices mentioned in WinCC. In plant operation, MindSphere connection is included in STEP 7, WinCC, Startdrive. The symbol ✖ shows availability of function in software.[66]

5.2.3 Use cases of TIA and OPC UA

Communication between top floor and shop floor is performed by TIA. Operational technology and information technology produce huge amount of data, this data processing and dataflows are managed by TIA.[67]

Steps involved in integration of OT and IT are as follows:

First of all, defining standards is necessary to design production line. So that machine actions will be set, and integration of line is possible in factory. The tasks for machines will be defined by operators and communication standard will help in easy integration of lines and production factory. Second step is to design ideally required machines by using the specifications. Simulation is performed to reach ideal concept by repetition of simulations. Modularization plays an important role in implementation, and it includes robotic arms, conveyor belts etc. In third step, focus is on automation of factory and testing of concepts related to different fields of engineering is done. At this stage all concepts are checked virtually. Virtual commissioning performs tasks such as checking of technical specifications and validation of PLC code. This helps in managing errors at early stage. In forth step, required machines are available and integration of machines into line is done. At last stage OT-IT integration is done and data will be available for transparency in production processes. The optimized production and plant capacity usage is possible which enhance overall factory performance.[67]

Use case in industrial communication for factory level, line level

The OPC UA and TIA are used together to obtain production data throughout all stages of the factory. There is communication between machines to machines as well as total production lines. Horizontal and vertical connectivity is provided by TIA and OPC UA due to which data can be accessed from anywhere and at any time. TIA provides network where all systems in production factory are connected to each other. Industrial communication in siemens is done via SIMATIC OPC UA S7-1500. [68]

Use case of line integration

Machines are combined to form a synchronous line for production. OPC UA is used as standardized interface for data and this facility is provided by TIA. If there are various interfaces for data, then data exchange is hard. OPC UA companion specifications are mapped with industry standards. Siemens OPC UA modelling editor is used for connecting controller data to standardized interface. This allows exchange of data and machines are linked to line. All machines operate synchronously and control with single line controller. The advantages OPC UA in line integration are openness, flexibility.[68]

Use case of integration of OT-IT for data processing

Industrial Edge from Siemens uses data of machines profitably. Data is collected in real time from components in system. Collected data is processed and then used in artificial intelligence for designing of automation processes. Globally available edge devices are connected to central system (Edge management). So, problem solving is easy and solutions are given in new functions with one click. In this way productivity is increased with Industrial Edge Management. The advantages are linkage from automation to cloud, central system, new functionalities and updates.[68]

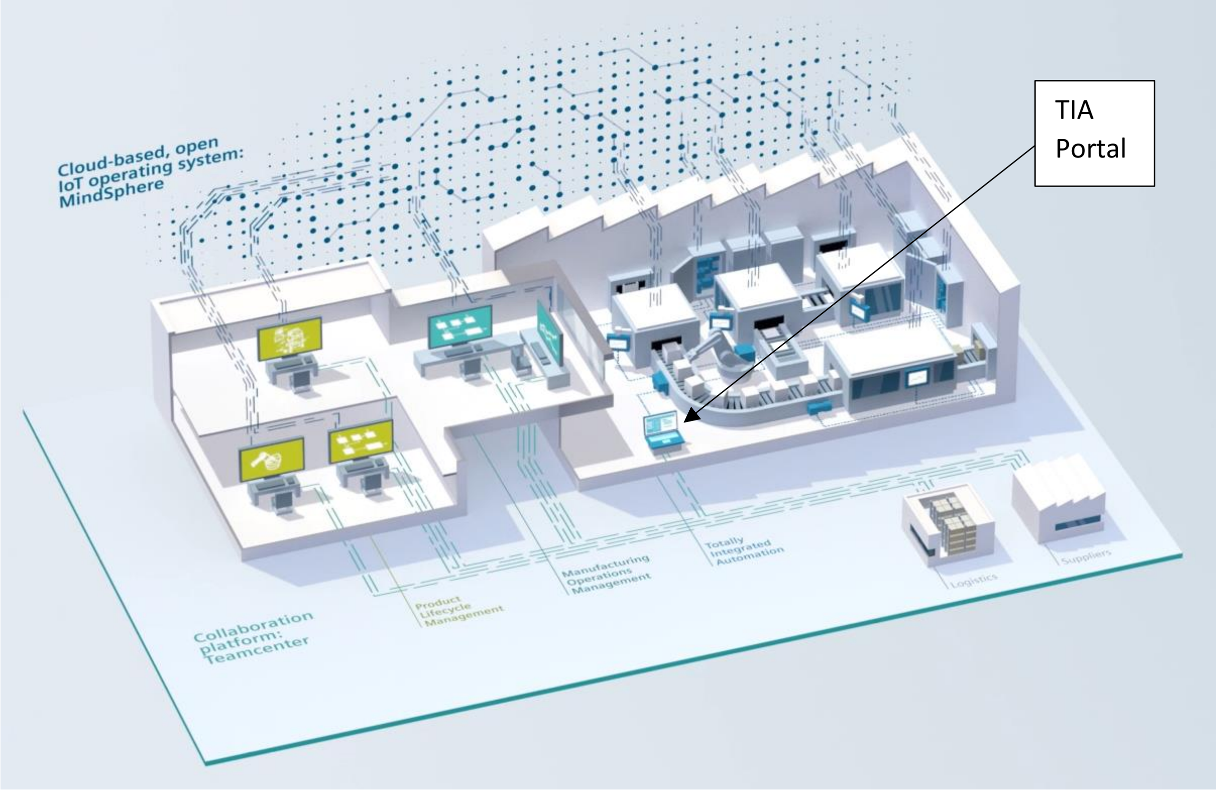

Cloud-based, open IoT operating system: MindSphere
TIA Portal
Collaboration platform: Teamcenter
Product Lifecycle Management
Manufacturing Operations Management
Totally Integrated Automation
Logistics
Suppliers

Figure 43: TIA in factory [68].

Use case in automation planning

AutomationML (Automation Amrkup Language) is standard and open format for exchange of data between electrical planning, hardware planning, hardware engineering. TIA Selection Tool is used to design hardware configuration. All configurations are stored in AutomationML file. Further this file is imported into ECAD systems for planning where there is no need of manual work. After planning in ECAD, import data to TIA portal. TIA portal provides continuous workflows and data exchange. The less time for planning is needed because of TIA portal and AutomationML.[68]

Use case in kinematics integration

Various kinematics are simply programmed and configured in TIA Portal from 5 to 6 axes. Single controller manages all tasks of automation. The system integration has kinematics up to 4 axes. Programming for movements in objects is set via SIMATIC HMI. Motion path is given to object via training in SIMATIC HMI. Motion path is validated through simulations performed in NX Mechatronics Concept Design, PLCSIM Advanced. There is no requirement of detailed knowledge during integration.[68]

Use case in interdisciplinary engineering

The fields used in planning of factory and machinery are mechanics, automation, electronics. These all fields are integrated into central application. Teamcenter database provides data consistently to all fields. Mechanical to well-designed mechatronic model is interconnected to electrical and automation model. Mechatronic templates can be reused and executed.[68]

Use case in supply chain management with RFID

The supply chain management with RFID provides total transparency in whole chain. Assets and containers, as well as other automation components, learn to interact with RFID readers and transponders. This allows for accurate identification and tracking of commodities along the value chain. PROFINET is used for PLC communication and control. Data about production and quality is sent to the transponder and transferred to IIOT systems like MindSphere through OPC UA. The data can be exchanged across business borders with all participants of the chain. The location, utilization and condition of all containers and assets is available total time.[68]

5.2.4 Practical example of TIA

The video from Automha Spa [69], mentions about using TIA, PROFINET and OPC UA together. Automha Spa is company located in Bergamo, Italy. The new technologies are integrated from Siemens in intralogistics sector and warehouses. TIA portal makes it possible to integrate services, software and hardware. The connections are provided in TIA by using PROFINET. TIA provides possibility to link applications which are present on horizontal level. Integration of these applications with remote systems is possible with TIA. Warehouses management systems are connected to cloud and factory systems via OT-IT integration. OPC UA standard is used for communication among cloud, warehouse management systems, factory systems etc. Company uses simulation software SIMATIC S7 PLCSIM Advanced with TIA portal and SIMIT for designing of processes and aspects related to safety.[69]

The SIMATIC controllers are part of TIA portfolio, and they are produced at Siemens Electronics Works Amberg. At this company, the production process is controlled and managed by TIA. Because of digitalization, the production boosted to 140 percent with similar use of resources and doubled complexity of product. The World Economic Forum (WEF) awarded EWA a Lighthouse Factory in 2021 for its excellent integration of digitization and automation, which resulted in several advantages. This award recognizes manufacturing facilities that have effectively used the industry 4.0 method to enhance productivity while also reducing environmental impact. Siemens produces around 1,200 product variants with over 17 million SIMATIC items each year. This example tells about role of TIA in industrial automation.[67]

Use case in Elster for OPC UA with SAP and production

The method to produce products is decided by products themselves. There is no requirement of manual preparation. The company Elster has assembly lines with production where they utilized concept of industry 4.0 successfully. The OPC UA is implemented with ERP, MES, and shop floor. The product is recognized by its individual shopfloor control number (SFC) at every stage. The management unit has direct connection to MES via OPC UA. Variables in PLC are converted to OPC tags and then these tags are mapped with MES interface. As a result, data exchange in complicated systems is rapid. The orders and completed items have QM characteristics stored in ERP system. Then these characteristics are accessed by MES. OPC UA is used as connector for factory and products.[60]

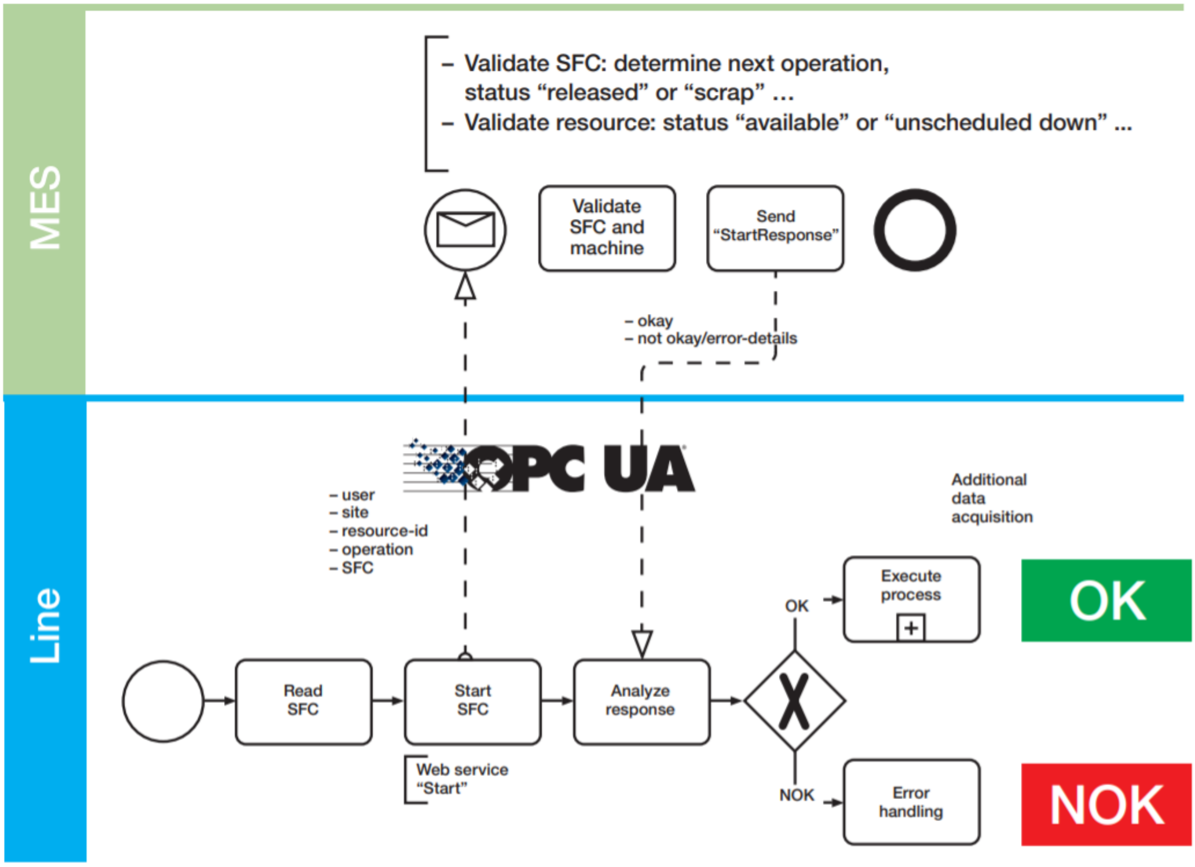


Figure 44: Dataflow in Elster [60].

Use cases explained by OPC experts

The expert has mentioned three use cases about IT/OT integration. The first use case is related to interface. There are different companies such as PLC vendor or machine vendor in which there is requirement of interfaces for integration. So, at this situation OPC UA is implemented. The interfaces are also required in various software such as HMI, MES. Software interfaces can be designed with the help of OPC UA. The other use case is related to aggregation of data. The aggregation server gathers data from sources and then combines all data to a OPC UA server. This improves the efficiency of communication between OT and IT applications with lowering communication overhead and cost. The aggregation server is used in applications to increase performance with simple maintenance. The third use case mentioned is about interface abstraction which might be applied to separate machines or in business area for separating locations.[62]

Use cases of PROFINET in Industry 4.0 by using OPC UA

The PROFINET is used for needs in engineering, redundancy and machinery initialization. The pair of OPC UA and PROFINET is convincing because this combination provides additional value for user. The practical examples for diagnosis and asset management are mentioned below.[70]

1) Asset management

Most of the users have no idea about devices which are installed in system over the time, and they also do not know firmware and hardware of installed devices. Asset management has requirements which are solved by PN-OPC UA Companion Specifications. Identification of asset is done by listing of all devices and controllers with parameters for network, submodules and modules, information about asset (vendor, version etc.), physical architecture for PROFINET network. The changes in assets are detected when there is update in firmware, new device, replaced device, physical architecture changes. The asset information can be changed by station name, tag function.[70]

2) Diagnosis

For smart diagnostic techniques, comprehensive information is also gathered from field. The strategies used in diagnosis are diagnostics of network (false neighbour), displaying of PROFINET connections, variations between actual assets and controller’s setup are identified.[70]

In following example, OPC server is installed in various devices such as Gateway, PLC, direct device integration. All field connections are provided by PROFINET and OPC UA is used for vertical communication.[70]

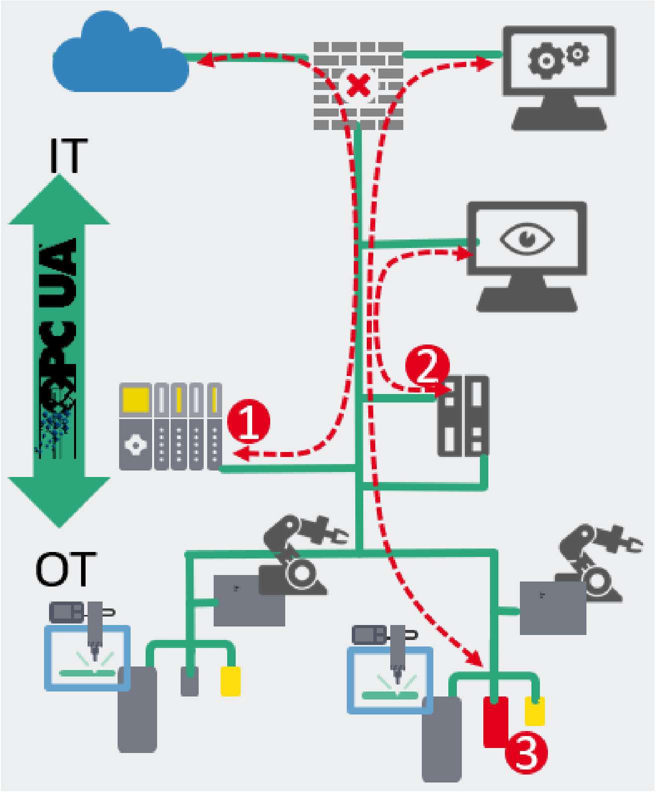


Figure 45: integration of OPC server in various devices [70].

In first case OPC server is installed into PLC. Cloud and PLC connection is established via OPC UA. In second case OPC server is installed in gateway. OPC UA is used to connect gateway and MES. In third case OPC server is installed directly in device, and vertical connection is established between device and upper level via OPC UA. This use case is good example of PROFINET, OPC UA.[70]

6 Discussion

The industry 4.0 is the fourth revolution which focuses on industrial automation. It has requirements which should be fulfilled to achieve smart factory concept. The communication between field level and control level is very important in automation. The PROFINET is solution for field level communication because of real-time communication, ability to connect field level data to cloud by using OPC UA. The PROFINET provides flexibility while designing the communication system. OT and IT are connected by using automation ethernet standard PROFINET.

The industry 4.0 requirements should be satisfied for achieving automation. In factory automation different manufacturers, various operating systems, multiple programming languages are involved. The connection with limited platforms has impact on scalability. If different platforms and devices are used in factory automation, then there can be problem of compatibility. The data security is important to avoid cyber-attacks. The transport and SOA are needed for various operations performed in industry 4.0. The integration of engineering tools and semantic extensions should be possible. The similarity with defined standards should be confirmed.

For all the above requirements, there is one solution which is universal protocol OPC UA. The communication provided by OPC UA is independent of industry sector. Multiple languages can be used in OPC UA protocol. The various devices like HMI, MES use OPC UA for communication. The OPC UA assures secure data transfer with standard verification. It supports different operations used in SOA and transport. The mapping of information to virtual models is done by OPC UA to observe real processes and products. The OPC UA is working with organizations such as PLCopen, AIM, AutomationML etc. for increasing integration in engineering and semantic extensions. The standard IEC 62541 is currently the OPC UA. It is used to confirm similarity of system.

Siemens TIA solutions combine advantages of PROFINET and OPC UA for industrial automation. The simultaneous communication between these two standards allows unlimited actions. From control level to cloud, the communication is done via OPC UA. The integration of different machines with various protocols is hard and complex. So, the single OPC UA protocol can be used with different devices. This saves time needed for industrial automation and productivity of plant is increased. The industrial automation specifications from OPC foundation are related to stacklights and statistical data. The visualization platform and manufacturing processes are linked with each other by using OPC UA, and this help in monitoring state of processes.

Totally integrated automation (TIA) is successful automation concept which is introduced by Siemens. The integration of hardware, OT, IT, various services, software is possible with TIA. The TIA portal is used in automation for simplifying the engineering tasks. It helps in digital planning, transparency in operations, various automation services. By use of simulation tools, the customers receive products in less time. The detection of problems, and energy management in plant is possible with TIA portal. The future technologies for automation are artificial intelligence, 5G, autonomous systems etc. The integration of these technologies with TIA portfolio is going on in Siemens. The WinCC, STEP7, Startdrive etc. can be integrated into TIA portal.

Therefore, TIA, OPC UA and PROFINET are used in industrial automation for various purposes from field level to cloud.

7 Conclusion and future work

The major topics included in this thesis are based on how the IIoT problems in intralogistics and production are solved by using OPC UA standard. The use cases and solutions are mentioned for understanding concepts used in industrial automation. The implementation of OPC UA standards to solve industry 4.0 requirements is also mentioned.

The IIoT/ Industry 4.0 has design principles which are real time ability, virtualization, interoperability, technical assistance, decentralization, modularity, information transparency. The advantages of industry 4.0 are customization, optimization, adaptability, profit, efficiency. The machine-to-machine and machine to cloud communication plays important role in industrial automation. Siemens introduced TIA for connecting software, hardware, services, future technologies, IT and OT. TIA is divided into three categories. The first category is integration of hardware, software, and services. The second category of TIA includes IT and OT integration. The third category of TIA mentions integration of future technologies. TIA is successful platform currently leading in automation. The use cases mentioned in thesis clearly show that TIA provides solutions for digitalization of factory. The Siemens control technology includes industrial communication, SIMATIC HMI, motion control etc. The industrial communication has various types of communications such as industrial ethernet, wireless industrial communication, industrial remote communication.

In this thesis, the OPC UA concepts and overview is explained in detailed. OPC UA specifications are mentioned for industrial automation. These specifications are focused on statistical data and stacklights. The standard framework is provided for statistical data and stacklights by OPC UA.

The needs of industry 4.0 are satisfied by using PROFINET and OPC UA. The OPC UA protocol is possible to implement in whole automation process. PROFINET is used for field level, while OPC UA manages M2M communication to cloud. The combination of OPC UA and PROFINET is used in Siemens for automation of plants.

So, TIA, OPC UA and PROFINET is excellent combination for plant automation. The use cases mentioned in thesis proved importance of OPC UA in IIoT.

In future, the specifications other than industrial automation specifications can be checked for detailed view of OPC UA specifications. The integration of OPC UA and TSN (time sensitive networking) into PROFINET is an interesting area for automation.

References

[1] A. G. Frank, L. S. Dalenogare, and N. F. Ayala, 'Industry 4.0 technologies: Implementation patterns in manufacturing companies', *International Journal of Production Economics*, vol. 210, pp. 15–26, Apr. 2019, doi: 10.1016/j.ijpe.2019.01.004.

[2] 'OPC UA speeds up the digitalization', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/opc-ua.html (accessed Dec. 28, 2021).

[3] 'A study of trends and industrial prospects of Industry 4.0 | Elsevier Enhanced Reader'. https://reader.elsevier.com/reader/sd/pii/S2214785321032417?token=351C824012DBE3F3D6F6DCD0EB2851CDB261812BA68382148632E1CB2EE0B901BB83FE374D9C40E586EF85C541CFC61F&originRegion=eu-west-1&originCreation=20210819193917 (accessed Aug. 19, 2021).

[4] P. K. Verma *et al.*, 'Machine-to-Machine (M2M) communications: A survey', *Journal of Network and Computer Applications*, vol. 66, pp. 83–105, May 2016, doi: 10.1016/j.jnca.2016.02.016.

[5] P. Drahoš, E. Kučera, O. Haffner, and I. Klimo, 'Trends in industrial communication and OPC UA', in *2018 Cybernetics Informatics (K I)*, Jan. 2018, pp. 1–5. doi: 10.1109/CYBERI.2018.8337560.

[6] 'Industrial Automation Siemens', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation.html (accessed Oct. 28, 2021).

[7] 'Totally Integrated Automation (TIA) seamlessly combines hardware, software, and services', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia/portfolio.html (accessed Oct. 28, 2021).

[8] '25 years of Totally Integrated Automation', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia.html (accessed Oct. 28, 2021).

[9] 'TIA-Integration 2', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia/it-ot-connection.html (accessed Oct. 28, 2021).

[10] 'TIA integrates future technologies', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia/future-topics.html (accessed Oct. 28, 2021).

[11] 'SIMATIC controllers – Take control of the future', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/systems/industrial/plc.html (accessed Nov. 09, 2021).

[12] 'Simply integrate machines into a line | Ingenuity | Siemens'. https://ingenuity.siemens.com/2019/11/simply-integrate-machines-into-a-line/ (accessed Nov. 09, 2021).

[13] 'Visualize future', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/simatic-hmi/wincc-unified.html (accessed Nov. 10, 2021).

[14] 'Machine level HMI', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/simatic-hmi/panels.html (accessed Nov. 10, 2021).

[15] 'SIMATIC WinCC RT Professional', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-professional-rt.html (accessed Nov. 10, 2021).

[16] 'SIMATIC WinCC V7 Basic Software', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-v7/simatic-wincc-v7-basic-software.html (accessed Nov. 10, 2021).

[17] ‘SIMATIC WinCC OA’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-oa.html (accessed Nov. 10, 2021).

[18] ‘SIMATIC IPC System’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/pc-based.html (accessed Nov. 10, 2021).

[19] ‘Industrial Communication and Networking’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication.html (accessed Nov. 11, 2021).

[20] ‘SIMATIC Technology’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/systems/industrial/simatic-technology.html (accessed Nov. 11, 2021).

[21] ‘Boosting productivity in CNC production’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/systems/cnc-sinumerik.html (accessed Nov. 11, 2021).

[22] ‘CNC-Systems’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/systems/cnc-sinumerik/automation-systems.html (accessed Nov. 11, 2021).

[23] ‘Safety Integrated for factory automation’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/safety-integrated/factory-automation.html (accessed Jan. 27, 2022).

[24] ‘Seamless integration of machine safety’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/safety-integrated/factory-automation/offering/simatic-safety.html (accessed Jan. 27, 2022).

[25] ‘3-63982-version-von-dffa-b10151-02-ws-simatic-safety-1-dffa-b101.pdf’. Accessed: Jan. 27, 2022. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:5d22a993-e055-4e88-a1ff-1ab66a3f3f05/3-63982-version-von-dffa-b10151-02-ws-simatic-safety-1-dffa-b101.pdf

[26] ‘Industrial Ethernet’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet.html (accessed Nov. 12, 2021).

[27] ‘Industrial Ethernet Switches - SCALANCE X’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/industrial-ethernet-switches-scalance-x.html (accessed Nov. 12, 2021).

[28] ‘fav-193-pd-pa-2016-en-web.pdf’. Accessed: Nov. 12, 2021. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:15079499-369a-40b2-a1d5-91f7388b522b/fav-193-pd-pa-2016-en-web.pdf

[29] ‘2018 - Production Network 4.0 - Modern network infrastruc.pdf’. Accessed: Jan. 28, 2022. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:ce56a714-7896-4c8a-b613-c3f13d4300c2/version:1559487657/fav-188-2018-pd-pa-en-web.pdf

[30] ‘Industrial IoT Gateways SIMATIC CloudConnect 7’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/industrial-iot-gateway-simatic-cloudconnect-7.html (accessed Nov. 12, 2021).

[31] ‘Best connections’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/system-interfacing.html (accessed Nov. 12, 2021).

[32] ‘FastConnect – cabling technology’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/fastconnect-cabling.html (accessed Nov. 12, 2021).

[33] ‘SINEC NMS’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/sinec-

networkmanagement/sinec-nms-network-management-system.html (accessed Nov. 12, 2021).
[34] ‘Network Security from Siemens’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security.html (accessed Nov. 12, 2021).
[35] ‘SCALANCE S Industrial Security Appliances from Siemens’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security/scalance-s.html (accessed Nov. 12, 2021).
[36] ‘SCALANCE M industrial routers’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/scalance-m-industrial-routers-ip-based-networks.html (accessed Nov. 12, 2021).
[37] ‘Security communications processors’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security/security-cps.html (accessed Nov. 12, 2021).
[38] ‘Industrial Wireless LAN’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-wireless-lan.html (accessed Jan. 05, 2022).
[39] ‘IWLAN_Logistics_OnePager_EN.pdf’. Accessed: Nov. 16, 2021. [Online]. Available: https://cache.industry.siemens.com/dl/files/648/109802648/att_1081868/v1/IWLAN_Logistics_OnePager_EN.pdf
[40] ‘SITRANS P280 | Pressure Measurement | Siemens Global’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/process-instrumentation/pressure-measurement/sitrans-p280.html (accessed Nov. 17, 2021).
[41] ‘SITRANS TF280 | Temperature Measurement | Siemens Global’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/process-instrumentation/temperature-measurement/sitrans-tf280.html (accessed Nov. 17, 2021).
[42] ‘Telecontrol’. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10095403?tree=CatalogTree (accessed Nov. 17, 2021).
[43] ‘Teleservice’. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10095417?tree=CatalogTree (accessed Nov. 17, 2021).
[44] ‘SINEMA Remote Connect’. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10357032?tree=CatalogTree (accessed Nov. 17, 2021).
[45] ‘Introduction to remote networks’. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10215928?tree=CatalogTree (accessed Nov. 17, 2021).
[46] ‘Remote Networks’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks.html (accessed Nov. 18, 2021).
[47] ‘siemens-ruggedcom-oman-pdo.pdf’. Accessed: Nov. 18, 2021. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:f8dfa3ce-44fc-4458-8a2c-017fb08a3958/siemens-ruggedcom-oman-pdo.pdf
[48] ‘RUGGEDCOM’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/rugged-communications.html (accessed Nov. 18, 2021).
[49] ‘RUGGEDCOM RMC’. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10167954?tree=CatalogTree (accessed Nov. 18, 2021).

[50] 'RUGGEDCOM Ethernet Switches Layer 2'. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10167955?tree=CatalogTree (accessed Nov. 18, 2021).

[51] 'RUGGEDCOM Ethernet Switches Layer 3 / Routers'. https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10167961?tree=CatalogTree (accessed Nov. 18, 2021).

[52] 'Process safety', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/safety-integrated/process-safety.html (accessed Jan. 27, 2022).

[53] 'Professional Services for Industrial Networks', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-network-solutions/professional-services.html (accessed Nov. 18, 2021).

[54] 'SINEC – Boost your network', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/sinec-networkmanagement.html (accessed Nov. 18, 2021).

[55] 'SINEC INS', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industrial-communication/sinec-networkmanagement/sinec-ins-infrastructure-network-services.html (accessed Nov. 18, 2021).

[56] 'What is OPC?', *OPC Foundation*. https://opcfoundation.org/about/what-is-opc/ (accessed Nov. 19, 2021).

[57] 'Unified Architecture', *OPC Foundation*. https://opcfoundation.org/about/opc-technologies/opc-ua/ (accessed Nov. 19, 2021).

[58] OPC Foundation, 'OPC Unified Architecture Part 1 :Overview and Concepts'. Nov. 22, 2017. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/

[59] OPC Foundation, 'OPC Unified Architecture Part 200 :Industrial Automation'. Jul. 31, 2021. Accessed: Dec. 11, 2021. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-200-industrial-automation-model/

[60] 'OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf'. Accessed: Dec. 27, 2021. [Online]. Available: https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf

[61] '-dffa-b10530-00-profinet-broschuere72dpi.pdf'. Accessed: Dec. 27, 2021. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:007470ec-18d0-4de0-9eef-5fd4b49744b0/-dffa-b10530-00-profinet-broschuere72dpi.pdf

[62] 'OPC Experts Interviews: OPC UA Use Cases', *automation.com*. https://www.automation.com/en-us/articles/september-2020/opc-experts-interviews-opc-ua-use-cases (accessed Dec. 30, 2021).

[63] 'sce-092-300-opc-ua-s7-1500-r1807-en.pdf'. Accessed: Jan. 02, 2022. [Online]. Available: https://www.automation.siemens.com/sce-static/learning-training-documents/tia-portal/advanced-communication/sce-092-300-opc-ua-s7-1500-r1807-en.pdf

[64] 'siemens-opc-ua-webinar-27aug2020.pdf'. Accessed: Jan. 02, 2022. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:d01f17aa-551e-4f68-9c55-93c6689c00ce/siemens-opc-ua-webinar-27aug2020.pdf

[65] 'TIA Portal', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html (accessed Dec. 28, 2021).

[66] 'Discover software in TIA Portal', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal/software.html (accessed Dec. 28, 2021).

[67] 'TIA lets you make the digital enterprise a reality', *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia/it-ot-connection.html (accessed Dec. 29, 2021).

[68] ‘Digitization Uses Cases | TIA IT/OT-Integration | Siemens Global’, *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/topic-areas/tia/it-ot-connection/tia-use-cases.html (accessed Dec. 29, 2021).

[69] ‘Learn more about intralogistics solutions from Siemens’, *siemens.com Global Website*. https://new.siemens.com/global/en/markets/intralogistics.html (accessed Jan. 27, 2022).

[70] ‘Vertical communication’. https://www.profibus.com/technology/industrie-40/vertical-communication (accessed Jan. 26, 2022).

List of figures

List of tables

Appendix - Terms and Definitions

AddressSpace	collection of information that a *Server* makes visible to its *Clients*
Aggregate	a function that calculates derived values from *Raw data*
Alarm	type of *Event* associated with a state condition that typically requires acknowledgement
Attribute	primitive characteristic of a *Node*
Broker	intermediary program module that routes *NetworkMessages* from *Publishers* to *Subscribers*
Certificate	digitally signed data structure that contains a public key and the identity of a *Client* or *Server*
Client	software application that sends *Messages* to OPC UA *Servers* conforming to the *Services* specified in this set of specifications
Condition	generic term that is an extension to an *Event*
Communication Stack	layered set of software modules between the application and the hardware that provides various functions to encode, encrypt and format a *Message* for sending, and to decode, decrypt and unpack a *Message* that was received
Complex Data	data that is composed of elements of more than one primitive data type, such as a structure
DataSet	list of named data values
DataSetMessage	payload of a *NetworkMessage* created from a *DataSet*
Discovery	process by which *Client* obtains information about *Server*s, including endpoint and security information
Event	generic term used to describe an occurrence of some significance within a system or system component
EventNotifier	special *Attribute* of a *Node* that signifies that a *Client* may subscribe to that particular *Node* to receive *Notifications* of *Event* occurrences
Information Model	organizational framework that defines, characterizes, and relates information resources of a given system or set of systems
Message	data unit conveyed between *Client* and *Server* that represents a specific *Service* request or response
Message Oriented Middleware	infrastructure supporting sending and receiving *NetworkMessages* between distributed systems
Method	callable software function that is a component of an *Object*
MonitoredItem	*Client*-defined entity in the *Server* used to monitor *Attributes* or *EventNotifiers* for new values or *Event* occurrences and that generates *Notifications* for them

NetworkMessage	*DataSetMessages* and header to facilitate delivery, routing, security and filtering
Node	fundamental component of an *AddressSpace*
NodeClass	class of a *Node* in an *AddressSpace*
Notification	generic term for data that announces the detection of an *Event* or of a changed *Attribute* value; *Notifications* are sent in *NotificationMessages*
NotificationMessage	*Message* published from a *Subscription* that contains one or more *Notifications*
Object	*Node* that represents a physical or abstract element of a system
ObjectType	*Node* that represents the type of definition for an *Object*
OPC UA Application	*Client*, who calls OPC UA *Services*, or a *Server*, which performs those *Services*, or an OPC UA *Publisher* or an OPC UA *Subscriber.*
Publisher	entity sending *NetworkMessages* to a *Message Oriented Middleware*
PubSub	OPC UA variant of the publish subscribe messaging pattern
Profile	specific set of capabilities to which a *Server* may claim conformance.
Program	executable *Object* that, when invoked, immediately returns a response to indicate that execution has started, and then returns intermediate and final results through *Subscriptions* identified by the *Client* during invocation
Server	software application that implements and exposes the *Services* specified in this set of specifications
Service	*Client*-callable operation in a *Server*
Subscriber	entity receiving *DataSetMessages* from a *Message Oriented Middleware*
Subscription	*Client*-defined endpoint in the *Server,* used to return *Notifications* to the *Client*
Variable	*Node* that contains a value
View	specific subset of the *AddressSpace* that is of interest to the *Client*