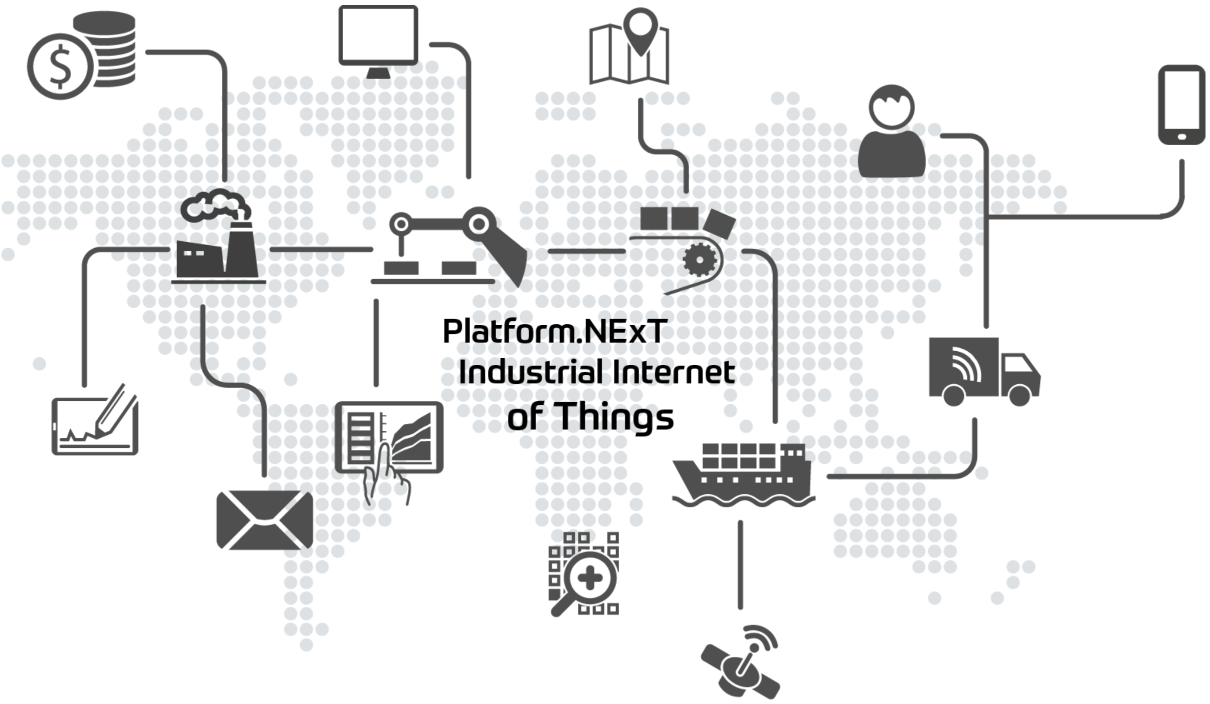
Automation
Platform.next™

IIoT: Industrial Internet of Things with Platform.NExT™

The growing demand for industrial connectivity, in line with Industry 4.0, requires solutions based on the idea of Internet of Things, and thanks to Automation Platform.NExT™, cutting-edge IIoT (Industrial Internet of Things) technology provides simple, effective solutions.



Nowadays everyone is talking about connectivity. Indeed, in the world of modern automation, communication is a vital factor for systems – no matter how different or faraway – to share data, which is the key element allowing companies to make quick, effective choices for improving efficiency and quality, and thus for having the edge in today's global market.
However, the topic of communication is extremely varied, complex and fragmented. Most people talk about "Industry 4.0", or IIoT (Industrial Internet of Things), or M2M (Machine to Machine), Telemetry, Big Data and more. All those terms identify similar though different notions, and operational contexts are extremely fragmented, stemming from different standard types, using different hardware systems, protocols and software platforms.
Also, generic wording used in marketing communication can be misleading. Of course, some of these ideas have been around for a while: the gathering of field data, even from remote locations, is currently used by more advanced

companies. So why is there so much talk about IoT and Industry 4.0? And is it possible to design suitable connectivity projects using existing, standard infrastructures, without investing huge resources?
First of all, let us take a closer look at terminology.

Industry 4.0

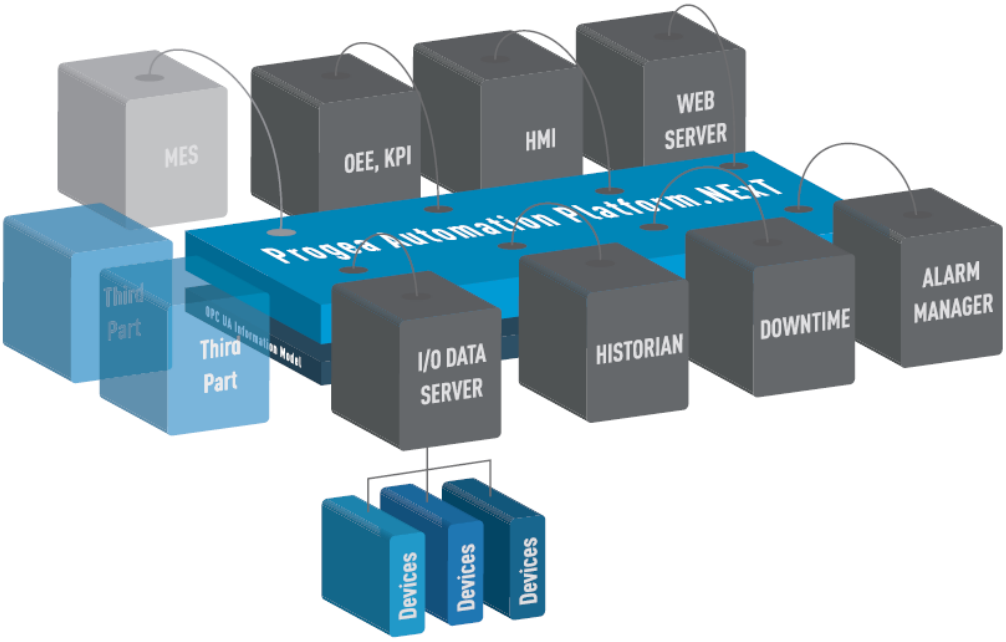
The term Industry 4.0 originated in 2011 from a strategic, tech-based project backed by the German Government, aimed at promoting digital transition and connectivity in the manufacturing industry as a strategic process of the fourth industrial revolution. The first industrial revolution is considered to have happened in England with the use of steam machines. The second industrial revolution was marked by the introduction of electricity in mass production, whereas the third industrial revolution saw the introduction of computer systems for production purposes.
Therefore Industry 4.0 is no actual technology, but rather a strategic plan made of implementation steps and guidelines for using the most advanced connectivity technology in order to create what are known as Smart Factories.
Such a generic idea can include several different technologies, e.g. Ethernet, Internet, Cloud, Databases, or any other system ensuring the data flow from sensors to management systems (MES/ERP).

M2M

The term Machine to Machine (M2M) usually is defined as direct connectivity between two devices or machines – usually by means of a wireless system – aimed at ensuring direct management of local devices, each performing its function independently.
In order to obtain such connectivity, 'point-to-point' systems are used, whereby essential data is transferred from one machine to another by means of a modem or other wireless device.

Internet of Things

The term "Internet of Things" (IoT) was invented in the early 2000s envisaging a global network of objects linked to one another, using the Internet to grant easy access to each entity, overcoming M2M's limitations and expanding its potential, so that each connected device can share data with its device group, or receive commands from it.
This type of connectivity has opened the door to huge possibilities, with the potential to redefine the notion of 'smart' devices, both for daily use (Consumer) and industrial use (Business). As concerns industrial use (IIoT), which is much more valuable and strategic, some extra criteria as compared to standard connected systems must be taken into account, such as security and reliability.



Modular platform concepts for IIoT and data analysis solutions with Platform.NExT

IT/OT convergence

Through widespread connectivity, a huge amount of data will be available for businesses to use, a true revolution opening the door to scenarios that were unthinkable until recently, requiring careful evaluation and analysis so that available data is effectively used by making the most of infrastructures and data flows. Suffice it to think that according to some estimates 10 billion devices will be connected within a few years from now, so it is necessary to select the data that needs to be shared, in order to avoid overloading networks with data, or acquiring data that ultimately will never be read.

The availability of information at any business level leads to the great benefit of overcoming the split between OT (Operational Technology) and IT (Information Technology). The convergence of these two strategic aspects of a business is a great revolution in itself, which will imply a change of approach to business management. This will create suitable synergy for IIoT projects, so as to substantially improve production efficiency, given that the ultimate strategic goal of information is to make better decisions, better yet if automated. That is where the real challenge of Industry 4.0 lies.

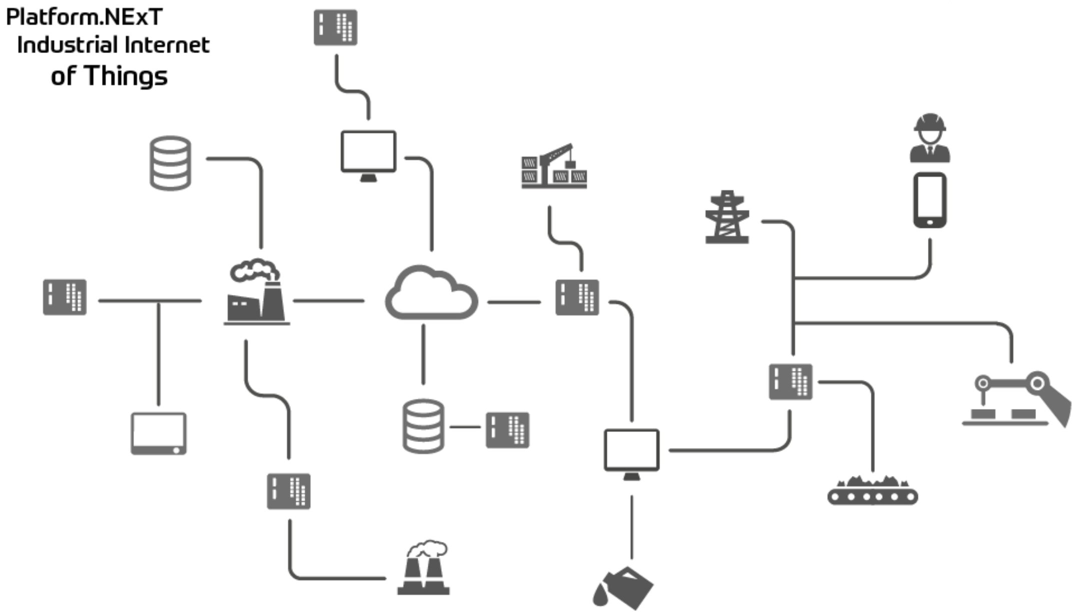
Let us briefly examine the basic ideas of IIoT technology using the Automation Platform.NExT industrial software platform.

IT-OT convergence and the importance of data

Typically, business managers who employ modern technology for their production processes know perfectly well that a sort of communication barrier exists between the IT (Information Technology) division and the OT (Operational Technology) division.
IT is generally involved with operating systems, databases, business servers, communication networks, and broadly speaking of processing data for planning, logistics and orders. On the other hand, OT generally deals with production-related processes, machines, equipment, as well as monitoring, supervision and maintenance systems such as PLC, RTU, CNC, HMI, SCADA. Both these divisions use technology in the workplace, though with different approach and different tasks, so that the potential of both divisions is often restrained, due to communication difficulties across such divisions. It is estimated that for many businesses, a significant share of data available at factory level (ranging from 40% to 80%) is completely unknown to IT divisions, which could manage processes more efficiently if they could access all data efficiently, consistently and in real time. Therefore, convergence between OT and IT, through the correct use of connectivity technology such as OPC UA or IIoT, may redefine business structures, and make business processes more integrated.

The importance of data

Data is crucial, that is absolutely no news. It is clear to anyone that a decisional process is as efficient as it can be based on actual, real-time data. At factory level, this has been known for some time now, so OT operators are used to managing data flow from PLC to SCADA, in order to ensure efficient production.

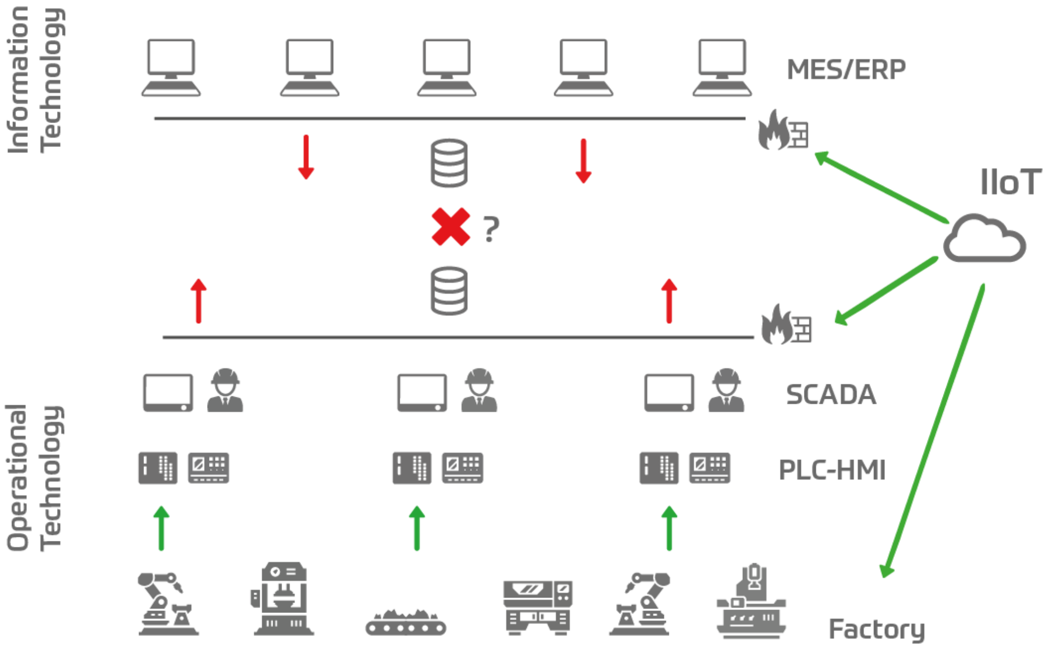


Such data, however, often stays at factory level (OT), and only part of it – somehow – reaches IT operators, who must manage decisional processes such as production planning based on orders, logistics and warehouse management, or administration priorities.

The Industrial IoT technology provides the possibility to ensure a more effective information flow, overcoming limitations and barriers between OT and IT business areas.

Moreover, it should be considered that horizontal connectivity may be required, i.e. data sharing may be required within the OT division only (different production systems interacting with each other), or within IT only (management systems interacting with each other) or both. IIoT technology was designed for overcoming any sort of infrastructural limitation.

At any rate, this type of technology requires a carefully assessment of needs, field technologies available, volume of data to be processed, reliability of infrastructures, performance and security. In order for an IIoT project to be fully functional, OT and IT's full co-operation is vital, so that each division's competences, know-how and expertise can translate into an achievement for the company.



The diagram shows the common split between OT and IT sides. An IIoT project makes it possible to overcome any communication barrier, even if location-based.

The following aspects constitute basic requirements:

1. **Communication protocols**
2. **Security and reliability**
3. **Software platform for the IIoT**

1 Protocols for communicating using the Industrial IoT

An IIoT project is based on the connectivity of different types of systems and devices, which may use very different data types and may be located at considerable distance of each other, so that the Internet (public network) may be the only affordable option to connect them. The first question to ask is: how can devices understand each other?

It is known that, in order for devices to communicate, a connection infrastructure and a shared protocol are required. That, of course, is also true for an IIoT project, as IIoT by itself does not include a communication standard. Today there are several ways to implement an IIoT project. However, as usual when several solutions are at hand, making the right choice is crucial, once the most suitable protocol is selected, based on needs, field devices and data to be processed.

The ideal protocol for IIoT

When it comes IIoT solutions there is no ideal or standard protocol. There are different solutions, different protocols, as well as 'custom-made' solutions. When selecting a solution, it is important to make sure that the protocol used for data exchange is as open, standard, secure and flexible as possible, considering that an IIoT project may be continuously expanding, as data to be gathered typically changes and expands along with the evolution of business processes. Therefore, closed-end or proprietary solutions should be avoided.

In this respect, the most successful type of IoT communication technology will introduce the true added value of the Internet of Things, i.e. the protocol's '**Discovery**' function.

Indeed, it will be crucial for any 'object' included in an IoT to become part of it without the need to edit the configuration in any way. This function would allow adding an IoT device which should be capable of joining a group and be 'recognized' by the other devices of that group. The 'Discovery' function is not enabled in any protocol yet, however the OPC UA specification defines its properties, though not as final.

OPC UA

OPC UA technology is the most effective, established and standardized protocol in industrial automation, and is perfectly suited for blending OT and IT.

OPC UA technology does not simply consist in exchanging data between a client and a server, it is the essence of the principles of interoperability and connectivity of factory-related data, which constitutes the basis of **Industry 4.0** concepts.
One of the pillars of this approach consists in OPC UA's cross-platform technology including performance and security, so that OPC UA Servers are even directly embedded in monitoring devices. Also, the OPC UA specification is developed in collaboration with PLC Open, which allows for a data model shared with IEC61131-3 programming. But there is more: in April 2014 additional OPC UA functionalities were added in Function Blocks of IEC61131-3 controllers, so that controllers themselves can become smart units in factory IT communication, improving and simplifying data access at all levels, both halfway up (SCADA/HMI) and at the top of the pyramid (MES/ERP).
For instance, in a 'smart' network, each device or service must be able to initiate communication and to respond to other services' specific requests.

Therefore, a device (OPC UA Server) can exchange even complex data structures (information), both vertically and horizontally, with other devices connected to the same 'smart' network, from the lowest to the highest level of the IT pyramid, both locally and over the Internet or the cloud, thus enabling the Industry 4.0 and IOT (Internet of Things) criteria, which are the pre-requisites of forthcoming architectures of new-generation integrated systems.
For instance, in a production line made of several machines supplied by different manufacturers, machines may communicate with each other in a client-server architecture. And that is not all. A higher-level system, or a service, may invoke a method (a supervisor to machines, a MES management system to the supervisor unit or to machines directly), to activate a production recipe, for example, as efficiently as a single call for exchanging input and output parameters. Cross-platform and security features directly integrated in the specification ensure maximum interoperability and security at all levels, both locally and sorted by location.

- Pros: IEC Standard, cross-platform, secure, complete specifications for any data type. Also suitable for Low-Cost and Low-End solutions using Micro-Servers devices.
- Cons: Due to the comprehensive architecture, implementation can be elaborate.

MQTT

MQTT (Message Queuing Telemetry Transport) is a protocol based on TCP/IP and on the publish/subscribe model. It is designed to be open, simple, light and easy to implement. Such features make it suitable to the IoT, i.e. to being used where limited bandwidth is available or where the implementing system has limited memory or CPU capabilities. The protocol was developed by two American researchers in 1999, and it has now been certified as standard by OASIS (Organization for the Advancement of Structured information), who stated that the MQTT protocol is particularly suitable for IoT solutions.

- Pros: simple, open, independent, cross-platform.
- Cons: not very common, not considered as standard in the world of automation. Insufficient security.

PubNub

PubNub is a real-time global infrastructure, expressly designed for creating web, mobile and IoT solutions. Established in 2010 as a private company in the US, PubNub immediately sparked the interest of large corporations which have financed its development, making this infrastructure one of the most interesting, reliable and effective in real-time, web-based data exchange. The company has rapidly developed, and this solution has proven particularly effective, simple to implement and economical.

The idea behind PubNub is to manage an API publish/subscribe messaging service within their global network, consisting of a network of data centers located on the main continents (America, Asia, Europe). The infrastructure currently serves over 300 million devices and sends over 750 billion messages per month.

Through API management, or using PubNub's SDK, any application or any device can publish or authorize data using the infrastructure. PubNub's business model is IaaS (Infrastructure as a Service) and the service requires a pay subscription.

- Pros: real-time, fast, simple, ready-to-use infrastructure, cross-platform.
- Cons: proprietary infrastructure, subscription-based service (over a set threshold).

Azure IoT

Azure IoT is the solution offered by Microsoft for IoT and IIoT. It features the same architecture as PubNub, however it uses Microsoft's Cloud infrastructure – the Azure platform. Through that infrastructure, using specific, simple connectors, applications and devices can share information. The benefit of Microsoft's architecture is that it can be easily integrated to other common IT solutions – such as the SQL Server database for Azure – and many more Business Intelligence solutions. Therefore, using the Azure

IoT connectivity-based solution, data can be shared on the Cloud, using an existing infrastructure managed by Microsoft itself, who guarantee its reliability. Because it is rather IT-oriented, Microsoft have decided to collaborate with the OPC Foundation. An OPC UA connector for Azure has been developed, allowing for IoT connectivity between Microsoft Cloud and the world of industrial automation, where the OPC UA standard is widespread.

- Pros: Microsoft Azure infrastructure allowing for a wide range of IT-related uses, cross-platform feature, ready-to-use Cloud infrastructure.
- Cons: more suitable for IT than for OT, less simple than other solutions, proprietary infrastructure, subscription-based service.

2 Security and reliability

The notions of security and reliability are what sets apart the Industrial Internet of Things from the standard Internet of Things. Obviously, it is one thing to have a household light switched on or to adjust the office temperature based on notifications from sensors or users, and another thing to ensure the production efficiency of an industrial site where hundreds of people work, where millions of euros' worth of goods are manufactured every day, and where quality must be ensured, or it may negatively impact customers.

For the above reasons, industrial communication protocols require suitable security and reliability features, although still in the same context as IoT.

The golden rule of security

Regardless of the protocol, which of course should be secure and reliable, the golden rule of security lies in the project, and in process management. Even before data integrity, good project design comes into play, which must be based on the risk which a possible transmission or communication error may imply. The project designer should then implement verifications, controls, double security, redundancy, watchdogs and any other planning element to ensure the security of particularly hazardous operations, most of all those in which people may incur physical consequences (pharmaceuticals, transport, foodstuffs, beauty products, infrastructures, etc.).

Secure protocols

When choosing an IIoT protocol, it is important to consider the security level and the type of potential risk. For example, it should be evaluated whether the protocol uses any data integrity control criteria, whether it allows to encrypt messages in case sensible data is transferred, whether it exposes the devices to hacking attacks or other cyber-security issues. It must be remembered, however, that the higher the implemented level of security, the slower the protocol's performance will be.

Security with OPC UA

There is no doubt that the protocol ensuring the highest security is OPC UA.

USER AUTHENTICATION AND AUTHORIZATION

When establishing a connection, each user is identified by:

- X.509 certificates
- Username/password
- or Kerberos

That way, all common user administration systems – such as Microsoft Active Directory, for instance – are supported. Also, access rights (e.g. for value reading and writing) may be specified and edited for each individual user.

INTEGRITY

Message signature prevents any third parties from editing the content of a message. That makes it impossible for a potential hacker, for instance, to change the message content, setting a variable to a non-allowed value, or to a different allowed value than in the original message.

CONFIDENTIALITY

The confidentiality of exchanged data is secured by message encrypting. To this end, modern encrypting algorithms are used. Latest, more powerful algorithms may be added to an application in the future without changing the protocol, in order to meet future security-related needs. It is sufficient to sign messages for selected areas in order to prevent editing by third parties, whereas for other areas further message encoding may be implemented, so that they are unreadable by any third parties.

APPLICATION AUTHENTICATION AND AUTHORIZATION

OPC UA applications are identified by means of a software certificate. An OPC UA Client may be granted access to an OPC UA Server based on its software certificate, and then it may access information saved on the OPC UA Server. Using software certificates, an OPC UA Server can be configured so that it accepts communication from specific OPC UA Clients. Similarly, an OPC UA Client can verify the authenticity of the OPC UA Server's software certificate – just like a web browser would. Such behaviors may be configured, i.e. an OPC UA Server may grant the same access to each client, based on user rights.

Security with MQTT

The MQTT protocol introduced – with version 3.1 – some requirements that improve its security level, although this protocol is unable to ensure the same level of security and solidity as OPC UA. The use of the MQTT protocol, due to its lightness and simplicity, cannot ensure a high level of data security. The protocol may be used on SSL (independently of the protocol itself) or – being an open protocol – extra data management security features may be added, but that would make it non-standard and would further complicate things.

Security with PubNub and Azure IoT

Using PubNub or Azure IoT infrastructures ensures a good level of security, as they natively support AES and TLS/SSL security standards, and allow managing permissions and certificates for data transmission between devices or applications. Also, they include an Access Manager which simplifies managing publication and authorization of permissions between devices or applications. Lastly, PubNub ensures the servers' physical security by using its own SSAE16-based policies. The use of these functions, however, needs to be planned if APIs for infrastructure access management are used in a project.

At any rate, these solutions offer the benefit of not having to open any 'door', which is at the origin of any security issue.

3 Software Platform

The last factor – perhaps the most important – that needs careful evaluation for an IIoT project is choosing the software platform for implementing data access and data management. The software application for gathering and managing IIoT data may be developed autonomously, writing code based on one's needs – provided one has the competence to do it and the required time and resources not only to do it, but also to manage all steps of maintenance and development.

Generally speaking, enterprises tend to focus on their core business and prefer using standard, open, user-friendly platforms. This is a strategic choice for any business that wishes to wisely invest its resources, reducing initial cost to then manage ROI (Return on Investment) in the medium-long term, to develop and expand its projects, as managed data is found to be vital for making strategic business choices.

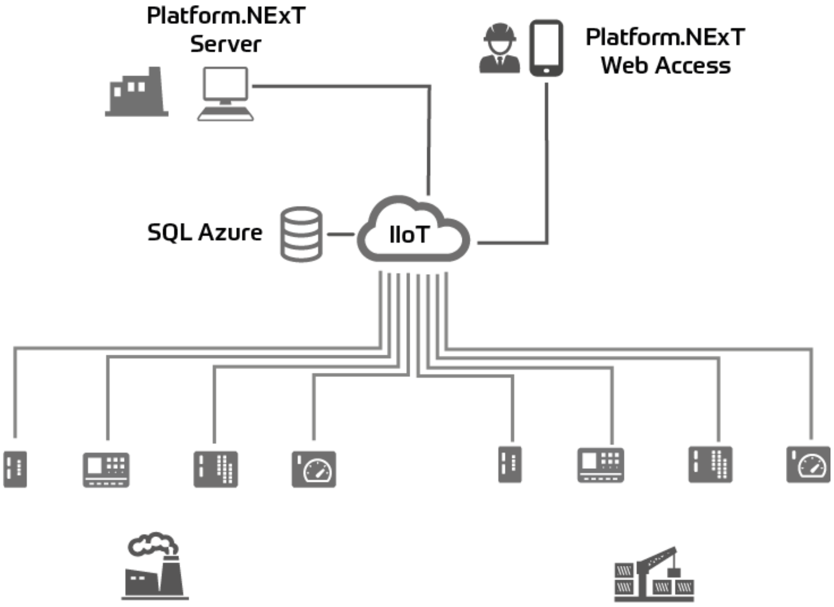
The ideal solution is a standard, open, user-friendly platform that gives the freedom to use the IIoT protocol or other industrial protocols, that is modular and expandable, and that includes all functions needed to add not only data gathering systems but also analysis, viewing, alerts, etc.

Automation Platform.NExT

Automation Platform.NExT is a new-generation software platform, based on the most modern and innovative software technology. It is developed by Progea, a company that boasts 25 years of experience in software technologies applied to automation, specifically SCADA/HMI platforms. Its most widespread product is Movicon, which boasts over 100,000 applications worldwide.

Automation Platform.NExT is a modular software solution, centered on a .NET framework especially developed by Progea for automation applications on PC-based architectures as well as on embedded systems. The platform uses the OPC UA data transfer specification, so that it constitutes a modular, open platform linking Client modules and Server modules in the same framework.

Thanks to its modular approach and technology, it is the ideal solution for IIoT projects, which need to be inherently open and flexible.



This diagram shows an example of data gathering from various field devices, connected in a single-protocol architecture for IIoT. The data gathering database in the example is Cloud-based (Ms SQL Azure)

I/O Data Server

Any IIoT project starts with data gathering. Hence, a server is required which can connect to devices, using the selected protocols. As concerns IIoT, Platform.NExT's Server natively features OPC UA connectivity, and can connect to any OPC UA-compatible device or application. However, it also has PubNub and MQTT protocols available, and it allows implementation of Azure IoT.

Moreover, the Server includes several other industrial protocols including Modbus, Siemens S7 TCP, Ethernet/IP, Omron, Mitsubishi, Profinet, IEC870, IEC850 and many more. That makes it possible to set up small gateway stations for local data gathering, based on proprietary protocols, and to publish required data using IIoT protocols on the company server.

Win10 IoT

A great feature of Platform.NExT consists in the power to create micro-projects of data gathering and data management using embedded devices such as Win10 IoT-based Raspberry PI. This option allows using local devices for locally managing digital and analog I/O, combining logics and sending data via PubNub or OPC UA to Platform.NExT's main server. Such a possibility hugely increases the platform's potential, offering a comprehensive, flexible solution to IIoT system designers.

Data Gateway

It is reasonable to assume that a data gathering and connectivity system that starts from installed field devices does not include on-board connectivity for IIoT solutions. If that is the case, it is necessary to set up a gateway solution, i.e. a device that can communicate with the existing protocol, and translate the required data over IIoT protocol, so as to ensure security and reliability. The above functions are featured in Platform.NExT's Data Server, which can function as a local gateway, communicate with field protocols and make the gathered data available on IIoT protocol, quickly and easily. The Data Gateway can also function as an OPC UA Server.

Historian over DB or over Cloud

Platform.NExT's Server includes a simple and powerful logging engine, which uses the Historian or Data Logger model. Server data can be saved on a database – typically SQL Server – as per default configuration. However, the system also supports Oracle or MySQL, or can save gathered data on the Cloud, as it supports SQL for Microsoft Azure.

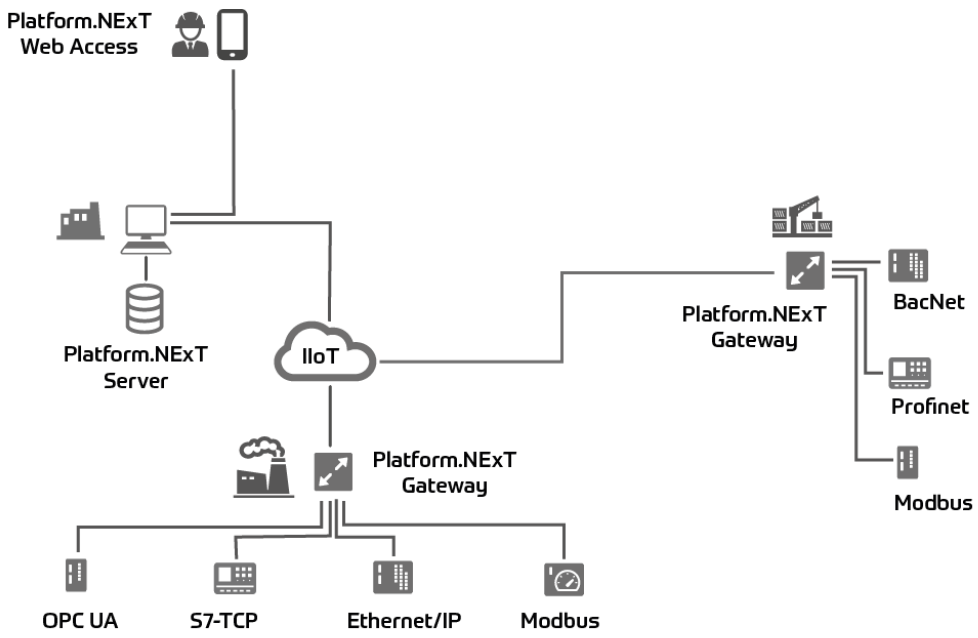
Therefore, Platform.NExT's solutions already includes all tools for transferring and collecting data, and for saving it in the database of choice, as per criteria and needs of a specific project.

SCADA, HMI and Data Analysis

Due to its modularity, the Platform.NExT platform also offers the possibility to flexibly and powerfully manage any Client side of an IIoT project. The platform's Client includes all HMI and Data Analysis functions for creating real time data presentations and even complex historical breakdowns, thanks to generous libraries of symbols and to the new-generation vector engine based on WPF (Windows Presentation Foundation) and XAML.

The client may be used locally – on a network or using web access – for viewing animated, dynamic synoptic tables, alert management, data trends and tables, charts, data analysis, dashboards and analysis reports.

Your IIoT project can turn into a true workstation for data analysis, supervision, MES, fully using all modules featured in the platform, including Movicon.NExT.



This diagram shows another example of data collection from various field devices, each of which in this case uses a different protocol. In this respect, Platform.NexT's Gateway function is the ideal tool for managing an IIoT project

Visit the website:

http://www.progea.com

Information on this document can be changed without prior information.

Progea Srl
Via S.Anna, 88/E
41122 Modena
Italy
Tel. +39 059 451060
Fax +39 059 451061
info@progea.com

Progea Deutschland GmbH
Marie-Curie-Str. 12
D-78048 VS-Villingen
Germany
Tel: +49 (0) 7721 / 99 25 992
Fax: +49 (0) 7721 / 99 25 993
info@progea.de

Progea International SA
Via Penate, 16
6850 Mendrisio
Switzerland
Tel:+41 (91) 96 76 610
Fax +41 (91) 96 76 611
international@progea.com

Progea USA, LLC
2800 East Enterprise Av.
US Branch Office
Appleton, WI 54914
Tel. +1 (888) 305-2999
Fax. +1 (920) 257-4213
info@progea.us