IIoT Applications

From nameplate via digital twin to asset health

Endress+Hauser

People for Process Automation

Content

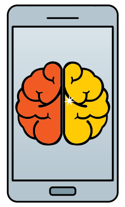
Introduction

Industrial Internet of Things

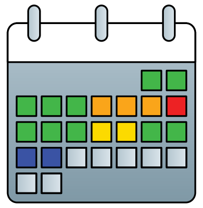
The typical domain of IIoT applications is manufacturing and production. Here the focus is on optimizing installed assets, especially to increase efficiency and availability. The ultimate goal is to predict future asset behavior based on historical data – often described as predictive maintenance or asset health monitoring. The majority of today's assets in processing plants already deliver much more information than just a single process value. This additional information can range from more process values to self-diagnosis about the asset's health or even the prediction, based on internally diagnosed device parameters, of potential problems that might occur in the near future.

This kind of information is often locked into the asset itself and can only be retrieved locally. The process automation plants that exist today are 5, 10 or even 20 years old and asset diagnostics was often not considered when they were planned. Although assets are replaced and new technology finds its way into existing plants over years of operation, the original integration of these assets into a PLC/DCS is rarely touched.

Thus, all the new device features and functions are not accessible without direct interaction with the asset itself. By changing this situation, the digitization and interconnection of all operational assets offers enormous potential for cost savings and optimization in the process industry.



Have the knowledge on your assets always with you



Track more information of your assets

Connect with your assets and further increase the potential

Jens Hundrieser
Regional Industry Manager Europe Metal
Endress+Hauser Messtechnik GmbH+Co. KG
Colmarer Str. 6
79576 Weil am Rhein| Germany

Steffen Ochsenreither
Business Development Manager IIoT
Endress+Hauser Process Solutions AG
Christoph Merian-Ring 12
4153 Reinach | Switzerland

Accessing asset information in existing plants

Unlocking the hidden potential

While the philosophy of IIoT is focused on unlocking the hidden potential of connected devices, that of existing plants is often exactly the opposite: locked down systems, with no means of connecting the installed assets. Furthermore, in order to make use of the features and functions of an asset, an overview about what is actually installed in the plant is required: where an asset is installed and what it can actually offer – although not all data provided are always of use.

When talking about IIoT, it is frequently said that data are required in order to create valuable insights. Although this is true, it is often forgotten that before this can happen, some important steps must be taken. Prerequisites to analyzing gathered data are knowing who the data provider is and what kind of data are to be accessed.

Without knowledge of the installed base and the data it will provide, analysis is practically impossible. In plants that have been around for a few years in particular, it is often not clear what the current installed base looks like.

- Who manufactured the devices installed?
- How many different device types are there?
- Are the devices still available or are some of them already obsolete?

Therefore, the first step into IIoT actually includes manual work: creating a list of all installed assets in a plant with at least some basic information such as manufacturer, asset type, location and a unique identifier (usually the serial number). Traditionally, this is done by sending a technician into the plant with a pen and paper, to document the serial numbers, the manufacturer, the asset type and other relevant information such as location etc. Afterwards the data are collated in a list and then the real work starts.

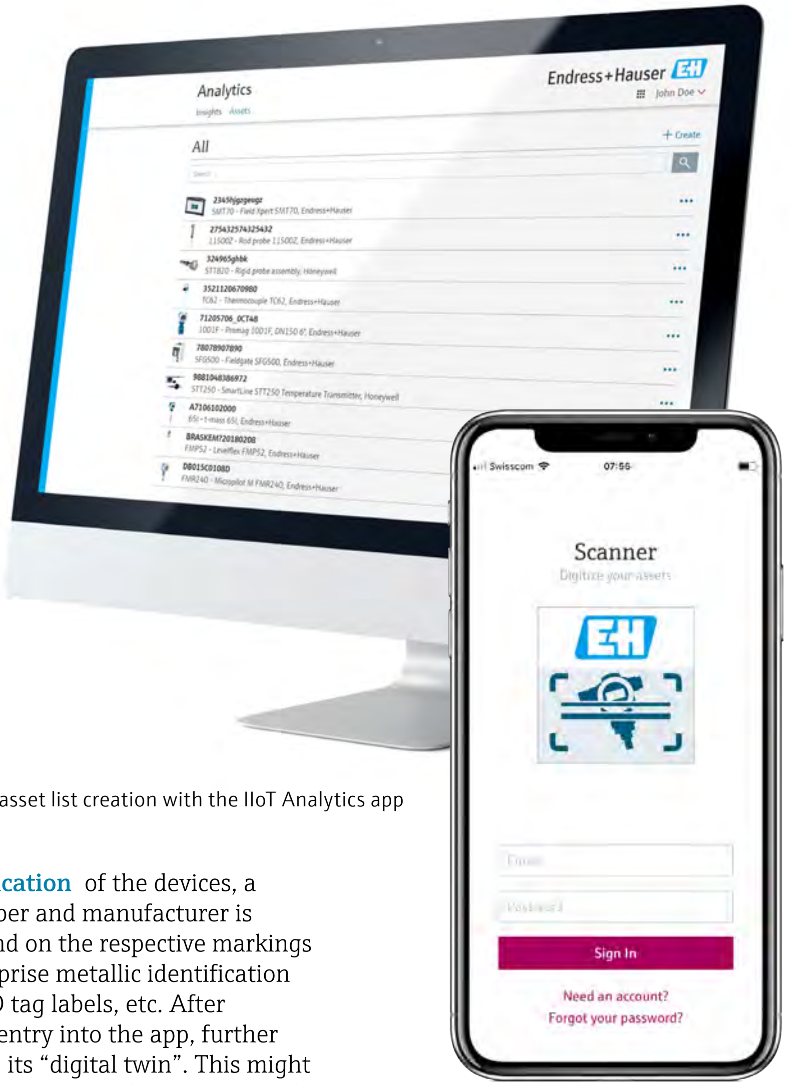
- Are the assets still available?
- Where can the documents, manuals, calibration certificates etc. be found? And so on and so forth!

Normally, reliance on existing plant documentation is not recommended: documentation on installed assets is often outdated or incomplete and can hardly serve as a basis for information gathering. There is usually no other way than to go through the system physically, to manually identify, capture, and create a new database. Obviously, this method of creating the database requires a great deal of time, effort and human resources. In addition, neither the data consistency nor the validity of the data is guaranteed. Although documenting the installed base is a crucial step towards the world of data analytics/IIoT, for many the entry hurdle is too high, as the time and money spent on manually creating a simple list of installed assets outweighs the benefits.

Automatic database creation and digital twins

It only takes a few steps

With the technology available today, this entry hurdle can be substantially lowered. Mobile devices can be used to create a device database with the help of Endress+Hauser's Analytics smartphone app. It takes just a few steps and in a matter of seconds.



Analytics
Insights Assets
Endress+Hauser
John Doe
All
+ Create
Search

2345hjgzgeugz
SMT70 - Field Xpert SMT70, Endress+Hauser

275432574325432
11500Z - Rod probe 11500Z, Endress+Hauser

324965ghbk
STT820 - Rigid probe assembly, Honeywell

3521120670980
TC62 - Thermocouple TC62, Endress+Hauser

71205706_0CT48
10D1F - Promag 10D1F, DN150 6", Endress+Hauser

78078907890
SFG500 - Fieldgate SFG500, Endress+Hauser

9881048386972
STT250 - SmartLine STT250 Temperature Transmitter, Honeywell

A7106102000
65I - t-mass 65I, Endress+Hauser

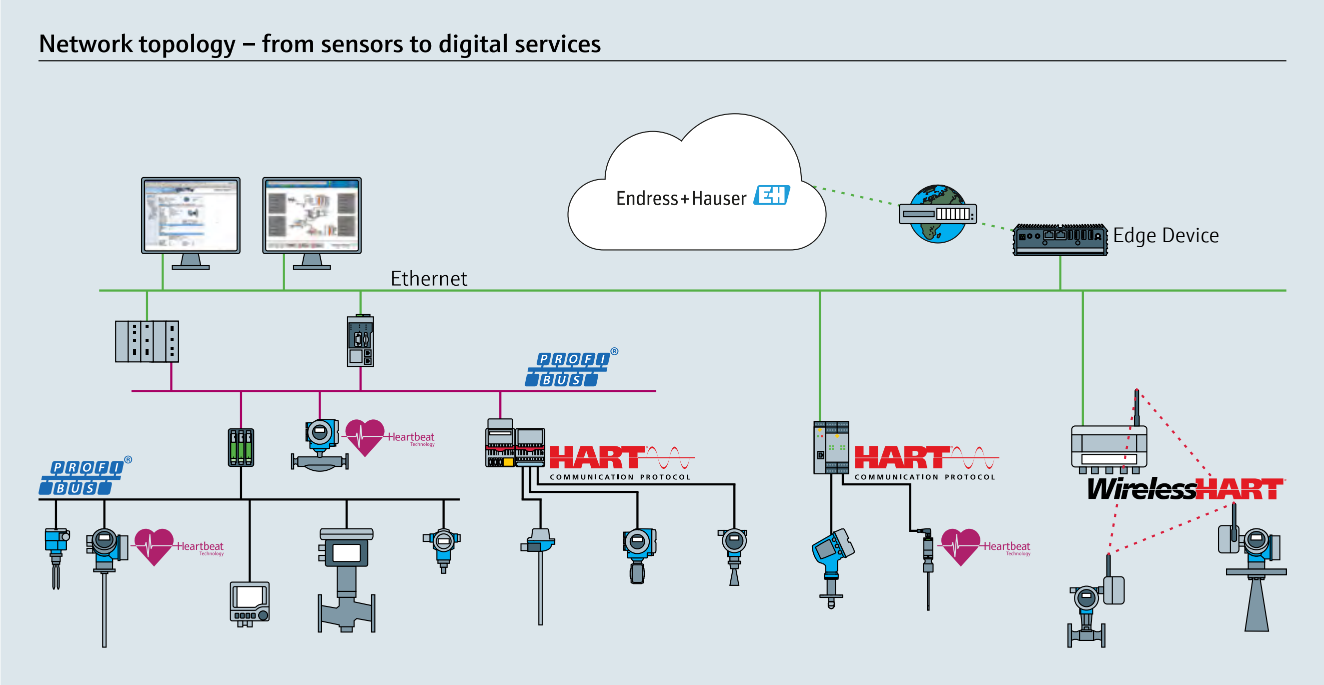
BRASKEM720180208
FMP52 - Levelflex FMP52, Endress+Hauser

D8015C0108D
FMR240 - Micropilot M FMR240, Endress+Hauser

Swisscom 07:56
Scanner
Digitize your assets
Email
Password
Sign In
Need an account?
Forgot your password?

Optimized asset list creation with the IIoT Analytics app

For the unambiguous identification of the devices, a combination of the serial number and manufacturer is usually used. These can be found on the respective markings of the devices, which may comprise metallic identification plates, QR codes or digital RFID tag labels, etc. After identification of the asset and entry into the app, further information can be attached to its "digital twin". This might be as geolocation (using the GPS functionality of the mobile device, for example), the tag of the asset, criticality and similar information, comments as well as photos and drawings of the instrument and its location. In tests with participants of different ages and education levels, the average time it took to gather all this information and create the database entry for a single asset was less than a minute. Obviously, in a plant with hundreds of assets, this still might become a tedious task.



Network topology – from sensors to digital services

PROFIBUS/HART network with edge device for automatic creation of asset database

Since the arrival of digital communication protocols such as HART, PROFIBUS and FOUNDATION Fieldbus, the goal has always been to provide the user with more information from the field and unlock the data and features that the manufacturers built into their devices. All these protocols provide a standardized means of reading the electronic nameplate of connected assets. By using an edge device Endress+Hauser has developed a means of accessing this information and transporting it to the Endress+Hauser cloud. This automatizes a major part of the manual work, massively reducing the effort required to create a digital twin of the installed base.

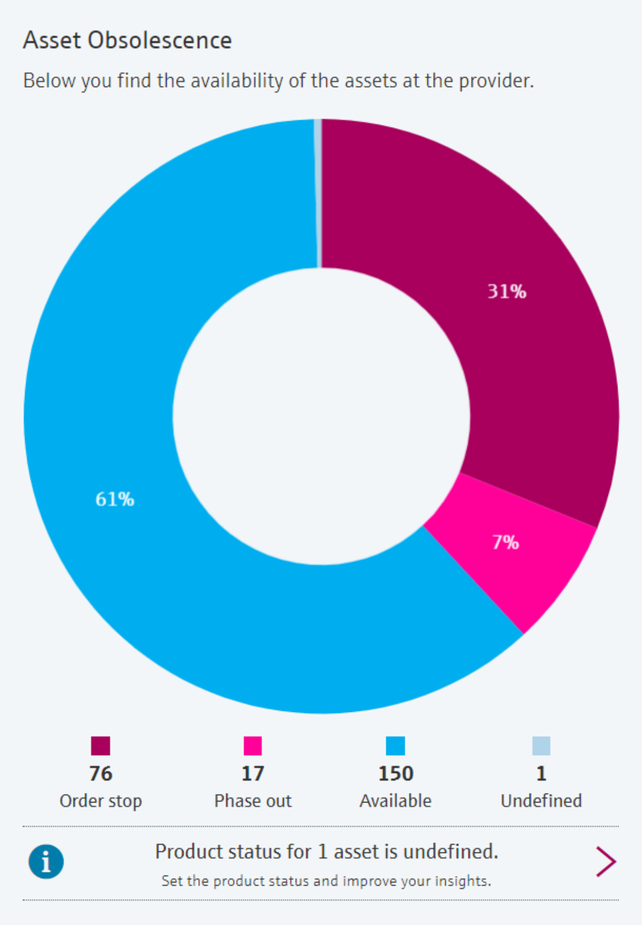
In field trials with selected partners, Endress+Hauser was able to automatically generate a database that included more than 800 assets in a single plant in less than 4 hours – from the installation of the edge device to the creation of the last digital twin.

But what happens next, how can the database be populated with additional data? Regardless of whether the database is created manually, via app or via the edge device, today's technology allows it to be connected to other databases, e.g. the manufacturer's asset information system. In the case of Endress+Hauser, this means device-specific documents such as manuals, certificates etc. are immediately at hand. Endress+Hauser's device database, the so-called W@M Portal, contains data records of no less than 47 million installed field devices. Account holders can also add information on any third-party devices to be found in their installed base.

This is very important as in today's process automation plants, the installed base often contains a large number of field devices from different manufacturers. To operate and maintain these plants economically, it is essential to have a comprehensive Plant Asset Management system. Studies have shown that up to 70% of the time required to complete a maintenance job is spent on searching for information - only 30% is spent on actually doing it. Considering that in older plants up to 30% of the installed base could be already obsolete, not having up-to-date information on its current status represents a big obstacle to the smooth running of the plant.

A big step forward towards successful asset management would be to simply make the user aware of the obsolescence situation. Luckily, Endress+Hauser's Asset Management system can easily provide this information even in a mobile app.

Here the obsolescence information is automatically generated in the database by cross-referencing the digital twin with data from the manufacturer's database. Having all this information at hand not only increases the efficiency of maintenance technicians, but also reduces the risk of faulty/inefficient maintenance, as the correct information is provided to the right person. This does, however, require a well-maintained and comprehensive device information database, which can be created as described above.



Asset Obsolescence

Below you find the availability of the assets at the provider.

🟪 76	🟥 17	🟦 150	■ 1
Order stop	Phase out	Available	Undefined

Product status for 1 asset is undefined.

Set the product status and improve your insights.

Visualization of asset obsolescence in a mobile app

Asset health

From static to dynamic asset information

Once the connection to the field has been established (via the edge device) and a comprehensive overview on the installed assets is available, the next step can be performed: the visualization of asset health. Thanks to Heartbeat Technology for example, the field devices are also able to output diagnostic values and device-specific trend parameters.

This asset data can be visualized to give users an indication of the availability of their assets. Gathering this information over a longer period of time and cross-referencing it with other process variables or external factors can then ultimately be used in a predictive maintenance application.

This is the logical step from static to dynamic asset information. Collecting and trending asset health over specific periods of time and storing this information in a database can ultimately lead to a collection of data which can then be used to forecast an asset's health.

Of course, all these additional asset management features and functions should never compromise the security and integrity of the actual process. By adding a bypass channel (through the edge device and e.g. the SFG500 Ethernet/PROFIBUS Gateway) to the asset management database, the PLC/DCS remains untouched. This offers multiple benefits:

- No additional programming of the PLC/DCS is needed to unlock the asset features
- Existing plants can be easily retrofitted without the fear of interfering with the existing process
- A bypass establishes another level of security, as asset management data is clearly separated from process data

Today's field devices often have the necessary connectivity to also transmit data directly to the database already built-in. This can be done by connecting through Wi-Fi, Ethernet technologies or even a mobile connection.

Security aspects

Take a look at the network architecture

In order to understand the relevant security aspects, it is necessary to take a look at the network architecture. This will give the entry points for the security discussion and show critical points of interest. The data flow starts in the field at the instruments. Via interfacing devices like gateways these data are transmitted into the cloud, where they are then transformed into information. There, additional data sources may be injected to create even more information. These can be other Endress+Hauser systems or customer environments such as engineering tools or ERP systems.

The connection to the asset management database has to be established in a secure manner. As shown, the edge device is located behind the company's firewall. As an additional security measure, the connectivity between edge device and Asset Management database is a one-way street. In this example there is no direct connection possible between the Asset Management database and the field network.

As security,trust and compliance are sensitive topics, a quality audit is essential. When the decision is to go for an IIoT offering, an accountable quality assessment of cloud services through a transparent and reliable certification process should be part of the process.

PROVIDED BY EUROCLOUD
EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM
Certificate
valid only if published on staraudit.org
★★★★
TRUSTED DIGITAL COMPETENCE PLATFORM

Any quality audit needs to consider different frameworks, laws and regulations that should include at least:

- ISO 27001: Information Security Management
- IEC 62443: Security for industrial automation and control systems
- Contract & Compliance
- Data Privacy
- Operational Processes
- Software as a Service
- ISO 20000: Service Management System

Functions and features To comply with all previously mentioned requirements, it is necessary to have proper functions and features implemented in the software. The following outlines some of the security measures that we undertake.

Encryption of passwords:
To provide user confidentiality of passwords we do not store them in plain text. At the user side passwords are encrypted with 'bcrypt + salt + pepper' and we just save the hash in our data base.

OAuth:
To support safe user identification during the usage of the software, we use a tokenized process to identify users against our cloud service. User passwords are transmitted only for token generation. This complicates scamming attempts and guarantees a safe authorization.

Encrypted communication channels only:
The communication channel to our cloud service is always established via a secure and encrypted https connection. Thereby all payload data are encrypted according to industry standards and our cloud computers are trustfully authenticated by a certificate issued by a worldwide renowned certificate authority.

User information:
When accessing his or her account the user is able to see past activities. The same mechanisms are used for online banking to detect possible fraud usage or failed login attempts.

Processes:
In the event of serious security incidents, which may occur in the safest environment, we have established internal processes to react as quickly as possible and to inform all affected parties to keep our customers safe from harm.

Server location:
We use the strongest cloud hosting partners in the world and only use server locations in Europe. These servers are operated under European law and jurisdiction, which is one of the most stringent in the world. Our customers can be sure that their data is subject to one of the highest data security standards worldwide.

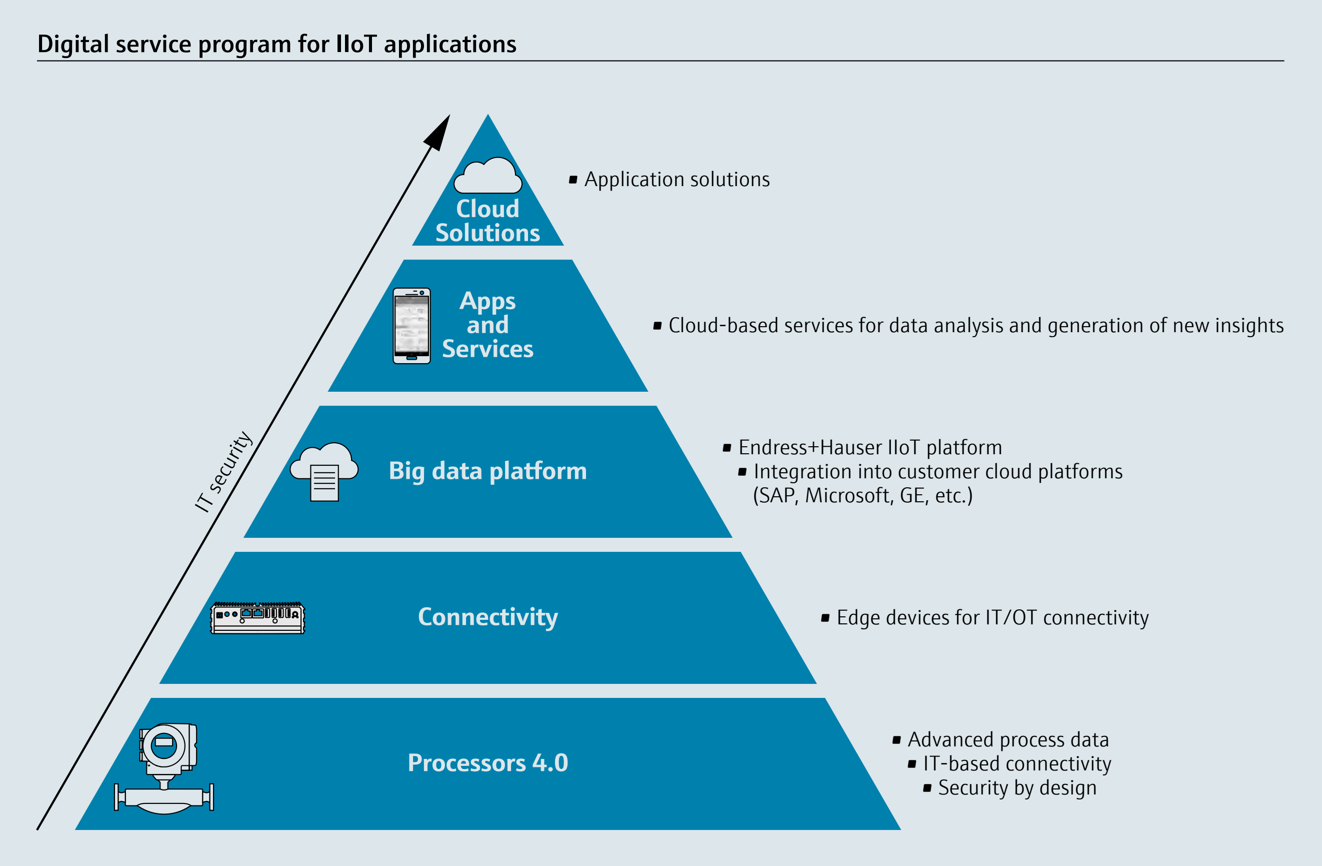
Gateway security:
The gateway is a critical point in the architecture because it represents the access point from and to the user's plant. The gateway will record only data from the field and transmit these into the cloud. Vice versa, i.e. from cloud to the gateway, no communication is initiated. Thus all incoming ports to the gateway are blocked. The only exceptions are software updates for the gateway. To guarantee safe downloads, these updates are certified and checked against the original file to prevent manipulation. Software updates are installed in parallel to the running system. When everything is complete the gateway is switched to the updated runtime and disconnected for the period of the reboot.

Customer data:
All customer data used by us are solely owned by the customer. We reserve the right to access these data to deliver our service. If we share customer data with 3rd party service providers, we inform our customers about this cooperation prior to data exchange and assure that this service provider acts according the given terms and guidelines.

Conclusion

Do things better

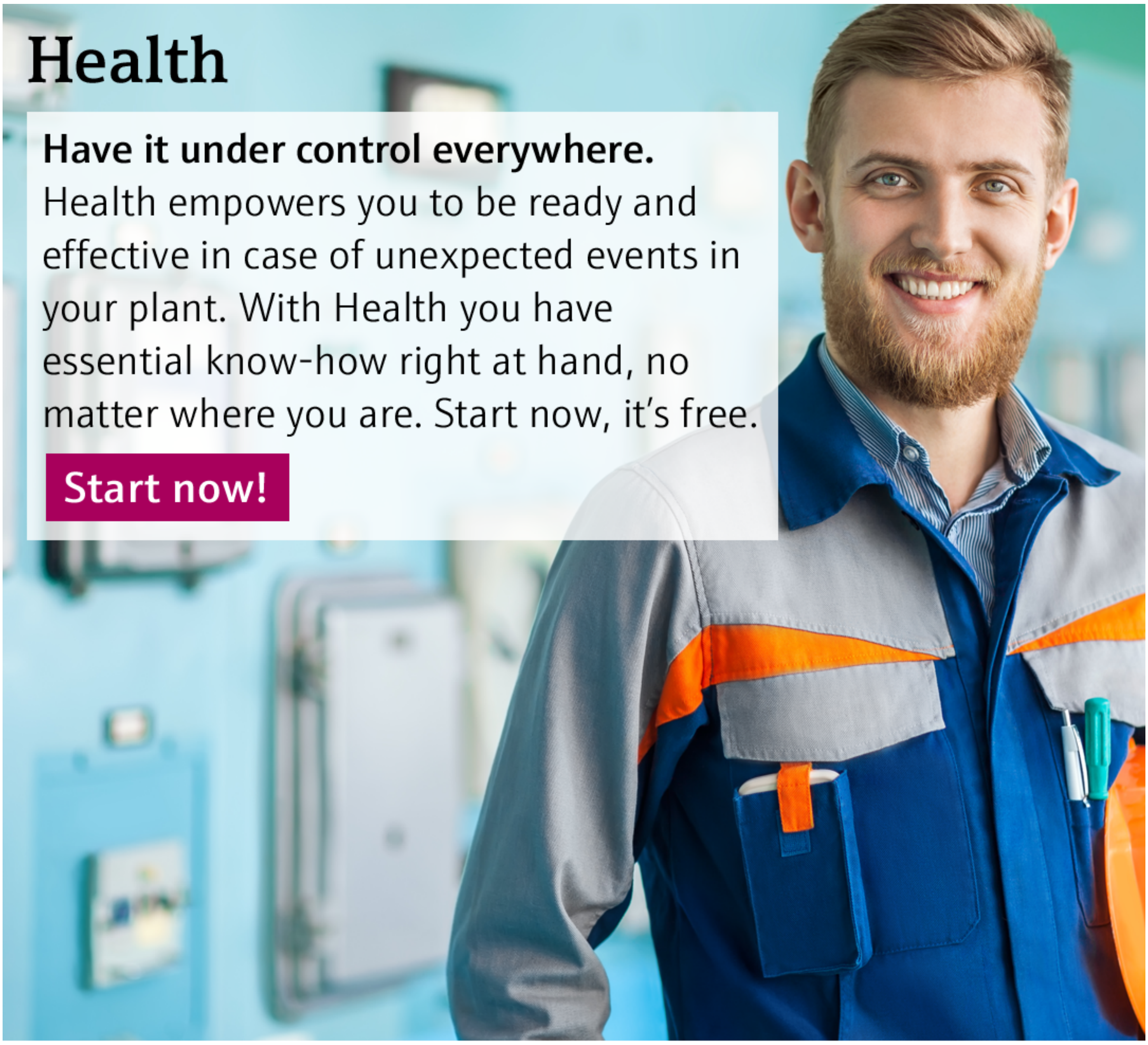
IIoT offers innovative ways in doing things better and utilizing assets that already exist. Customers can already benefit today from Endress+Hauser's IIoT services Analytics, Health and Library, which provide a digital service for the installed base.


Digital service program for IIoT applications
Cloud Solutions
Apps and Services
Big data platform
Connectivity
Processors 4.0
IT security
▪ Application solutions
▪ Cloud-based services for data analysis and generation of new insights
▪ Endress+Hauser IIoT platform
▪ Integration into customer cloud platforms (SAP, Microsoft, GE, etc.)
▪ Edge devices for IT/OT connectivity
▪ Advanced process data
▪ IT-based connectivity
▪ Security by design

Digital service program for IIoT applications

The installed base of a system can be simply captured and analyzed using real-time and historic data. Asset information in the field is recorded with a mobile smart device using the new Endress+Hauser Scanner app that reads an RFID chip, QR code or tag – alternatively, the asset information can be captured automatically by an edge device. All data are saved to the cloud, visualized on a dashboard, and asset management recommendations are issued, e.g. product availability or suggestions for a suitable replacement device.

In the near future Endress+Hauser intends to provide even more possibilities for connecting to devices and using data. Data security and privacy are a major concern, of course, but careful consideration when deciding for any IIoT solution can mitigate the risk. During the selection process, the IIoT provider should be critically reviewed and checked. Endress+Hauser has been audited by the non-profit organization EuroCloud StarAudit. This ensures the highest quality and security standards.



Health

Have it under control everywhere.
Health empowers you to be ready and effective in case of unexpected events in your plant. With Health you have essential know-how right at hand, no matter where you are. Start now, it's free.

https://www.iiot.endress.com/health

Eco-friendly produced and printed on paper from sustainable forestry.

www.addresses.endress.com

Endress+Hauser
People for Process Automation