DEVICE INTEGRATION STRATEGIES

Empowering the Intelligent Enterprise

CONTENTS

03. Editorial: Secure from the Core

05. FDT Solution Advances Industrial Cyber Security

12. Find Out How Endress+Hauser Makes Your Plant Intelligent

14. Fieldbusdevice.cloud for PACTware

FDT GROUP

What is FDT® Technology?

The FDT Group AISBL is an international non-profit corporation consisting of leading worldwide member companies active in industrial automation and manufacturing. The major purpose of the FDT Group is to provide an open standard for enterprise-wide network and asset integration, innovating the way automation architectures connect and communicate sensor to cloud for the process, hybrid and factory automation markets. FDT technology benefits both manufacturers and end users, with advancements such as the Industrial Internet of Things (IIoT) and Industry 4.0 delivered out-of-the-box – enabling modernized asset integration and access to performance data for visualizing crucial operational problems. Around the world, end users, manufacturers, universities, and research organizations are working together to develop the technology; provide development tools, support, and training; coordinate field trials and demonstrations; and enable product interoperability.

FDT Technology is comprised of two primary software components—the FDT Device Type Manager (FDT/DTM™) the driver for an intelligent device, and the FDT FRAME Application (FDT/FRAME™), which can be a stand-alone configuration application or embedded in engineering applications such as a DCS, PLC or asset management solution. DTMs developed by instrumentation suppliers provide a graphical interface to support configuration, diagnostics and troubleshooting of critical measurement devices and other assets. The FRAME Application provided by the system supplier, hosts DTMs used for management of all the devices on a wide variety of process and factory networks within a facility. Together, an FDT/FRAME and a collection of DTMs and/or other device drivers create an FDT-enabled application, which can be scaled from a small collection of devices to tens of thousands of devices controlled by a single FRAME throughout the automation communication pyramid.

Newsletter Contributors

CodeWrights

Endress+Hauser
People for Process Automation

SOFTWARE M&M
BY PEOPLE WITH PASSION
Member of WAGO Group

Rockwell Automation

Schneider Electric

utthunga
Engineering Transformation

wetcon
industrial it-solutions

YOKOGAWA

Learn More

>> FDT/DTM™ Catalog

>> FDT/FRAME™ Catalog

>> Newsletter Registration

>> Become a Member

>> Events

>> Contact Us

Visit **www.fdtgroup.org** for more information.

Join Us

LinkedIn

YouTube

Twitter

Editorial: Secure from the Core

Security team focuses on end-to-end information integrity

Lee Lane, FDT Group Chairman of the Board of Directors

I am pleased to report that our Architecture and Specification Working Group is making great progress on adoption of the .NET Core/Standard that will allow our new FDT® Server-based architecture to be completely platform independent. Additionally, I'm happy to report that our FDT 2.1 Common Component developer tool kits for FDT/FRAME™ and FDT/DTM™ development have been finalized and released, thus clearing the way to begin enhancing them for the FDT IIoT Server™ (FITS™) .NET Core/Standard technology for next-generation product development for the FDT Server and Web-based Device Type Managers™ (DTMs™).

As we prepare the emerging FITS standard for the market, one common inquiry we receive centers around data security of the Internet of Things (IoT). This is certainly understandable as we transition from primarily a single user, desktop standard to one that also supports browser-based Clients accessing an FDT Server deployed in the enterprise, on-premise or in the cloud. However, there is good news: From the beginning of FDT, security has been a central focus of our architecture and has grown with the adoption of a dedicated security team attentive to the implementation of a secure core design approach for the emerging FITS architecture. Having this team focused on nothing but security frees them from the burdens of developing the standard, in order to remain singularly focused on defining risks, threats and best practices to meet the use case requirements for quality assurance for security.

In prior versions of the FDT standard, we have always had a user authentication requirement and granted authorizations to the user using a role-based security model. This has served the end user community and our developer community very well over the past decade. The role-based security model will be retained and enhanced in the core of the FITS architecture by adopting a layered security approach based on the defense-in-depth strategy as the architecture becomes more distributed. As a result, we have added Server and Client device authentication as well. These X.509 certificate-based authentication schemes use industry standard Transport Layer Security (TLS) to confirm that not only is this the correct FDT Server, but that the Client device is also authorized to communicate

with the Server. This “triple handshake” of Server, Client device, and end user authentication ensures that no impersonations, man in the middle attacks or otherwise unauthorized access is permitted.

Additional provisions have been made so no one can eavesdrop on any of the communications. Again, we turned to well-tested TLS to encrypt all Client and app communications with the Server, in both directions, to ensure ultimate privacy.

For our OPC UA Server built into the FDT Server architecture, we support all security mechanisms that are prescribed by the OPC Foundation.

Finally, as a Server-based architecture, the ability to deploy the FDT Server in the public or corporate cloud allows full replication of the Server environment for instant cut-over in the event of a virtual Server or network failure. This improves availability, as all communications between a remote Server and the local control networks is conducted through a Virtual Private Network (VPN) tunnel or equivalent in order to shed the most nefarious of intrusion attempts.

This edition of our newsletter has a more in-depth look at security. I hope you will agree with me that our FITS architecture is engineered from the ground up to give you the assurance of a secure deployment. While we are happy with the progress so far, we remain committed to continued review of best practice implementations to ensure comprehensive data security.

FDT Solution Advances Industrial Cyber Security

FDT Server-based architecture enables comprehensive data security for IIoT applications

Industrial security is a complicated, multifaceted challenge that cannot be solved by simply purchasing the latest technology. Instead, managing the security of industrial control systems and networks requires improving processes, tools and ultimately balancing risk.

All too often, individual Personal Computer (PC) users are the attack vectors responsible for eventually compromising an industrial facility's entire automation infrastructure.

The advent of the Industrial Internet of Things (IIoT) has dramatically impacted the cyber threat landscape. The convergence of Informational Technology (IT) and Operational Technology (OT) has also complicated industrial security in some ways. Some organizations in the critical process industries have an air-gapped requirement prohibiting users of OT systems from direct or even indirect connection to the Internet. These organizations must find ways to safeguard data access from the enterprise all the way down to the device level.

Progress of the FDT Standard

Introduced in 1998 by FDT Group (an independent, international, not-for-profit standards association), FDT® technology (IEC62453, GB/T 29618-2017 and ISA103) standardizes the communication and configuration interface between field devices and host systems. It is regarded as the de-facto integration and information exchange standard and is deployed by millions of end-users around the world.

Integration resides at the heart of any automation architecture, and FDT provides a robust solution for the integrated manufacturing enterprise due, in part, to its strong security capabilities. The

Continued

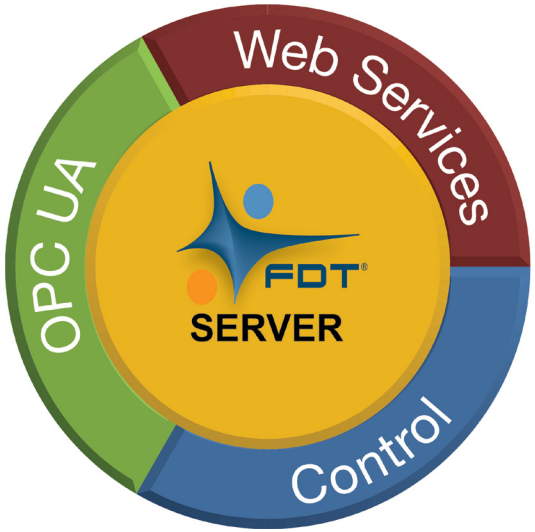
FDT Solution Advances Industrial Cyber Security

standard's comprehensive cyber security infrastructure addresses potential cyber-attacks on automation assets. FDT provides unparalleled protection when integrated in control system vendor applications and hosted within a secure IT platform.

Developing an IIoT Server Platform

In 2018, FDT Group announced the development of an FDT IIoT Server™ (FITS™) architecture that will provides a flexible platform for deployment of IIoT-based solutions. The emerging FITS specification is set to empower the intelligent enterprise with native integration of the OPC Unified Architecture (OPC UA), as well as Control and Web Services for mobile applications. FITS will enable cloud, enterprise, on-premise, and single-user desktop deployment methods to meet the needs for process, hybrid and discrete manufacturing.

The FDT Server architecture allows for integration of web-based Device Type Managers™ (FDT/DTMs™) that are digital representations for physical devices. The FDT Server will include an online repository providing end-users with convenient access to the DTMs they need for various applications. The solution also includes an OPC UA Server, WebServer and stand-alone (local) applications.



The OPC UA Server allows access to DTM data with OPC UA Clients. The WebServer enables the use of DTM WebUIs on remotely connected, web-based clients on smart phones, tablets, and PCs. The WebServer also supports the use of apps that improve workforce productivity and plant availability.

FDT Group's Architecture and Specification Working Group is integrating the .NETCore/Standard to allow the new FDT Server-based architecture to be completely platform independent. This transition will result in an FDT Server architecture that is deployable on a Microsoft-, Linux-, or macOS-based operating system, which will empower the intelligent enterprise by bridging the current installed base with next-generation solutions supporting the IIoT and Industry 4.0 era.

Enhancing Security Performance

As FDT Group prepares the emerging FITS standard, an important consideration is data security for the IIoT. This issue has gained importance as FDT transitions from primarily a single-user and client/server application to a full distributive architecture that supports browser-based clients accessing an FDT Server deployed in the enterprise, on-premise or in the cloud.

FITS will help to do away with the traditional automation pyramid. Indeed, it provides a way to "flatten" the control architecture to eliminate barriers to plant applications in need of directly accessing lower level devices in order to acquire data for analysis, operational dashboards, etc. This is made possible through flexible and distributed components designed to minimize potential security risks.

The FITS solution was also designed to meet both connected and air-gapped requirements, support virtually any automation architecture, and comply with contemporary security policies in a typical industrial operation. Furthermore, it has the unique capability of authenticating client devices attempting to connect to the server.

Developed by the FDT Group Security Team architects for consistency across different operating system platforms, FITS features robust multi-layered security and leverages vetted industry standards such as Transport Layer Security (TLS) enabling Web Sockets Secure (WSS) and Hyper Text Transfer Protocol Secure (HTTPS). The FITS security strategy encompasses:

- Encrypted communications using TLS
- Role-based user security
- 509v3 certificates for authentication
- On-the-wire-security for enabled industrial control protocols

Continued
FDT Solution Advances Industrial Cyber Security

TLS is a cryptographic protocol designed to provide communications security over a computer network. It has three basic functionalities: message encryption, detection of message alteration, and authentication between client and server. TLS ensures that all communication exchanges are fully encrypted. This enables the exchange of sensitive information while mitigating the risk of interception or alteration.

The FITS security architecture offers an optional level of security rarely seen with consumer grade TLS implementations. In addition to standard encryption and server authentication, FITS can be configured to confirm that a specific client device is authorized to communicate with the server. From an IT/OT perspective, administrators can therefore ensure that authenticated client devices have appropriate virus protection and meet other corporate security guidelines to ensure they are not the source of contamination via connection to the server.

Any authorized browser, app or application connected to the FDT Server utilizes Web Sockets, and as such, will be protected by Web Sockets Secure. WSS ensures the same depth of protection through message integrity, message confidentiality and strong authentication. At the same time, HTTPS is the secure version of Hyper Text Transfer Protocol (HTTP) over which data is sent between a browser and the FDT Server to which it is connected.

In prior versions of the FDT standard, there has always been a user authentication requirement that grants authorization to users based on a role-based security model. This approach has been effective for many years and is credited with eliminating a huge administrative burden on industrial OT organizations. Role-based security will be carried forward in the core of the distributed FITS architecture as a multi-layered security approach employing a defense-in-depth strategy. This layering of multiple security mechanisms provides a robust “belts and suspenders” approach to security.

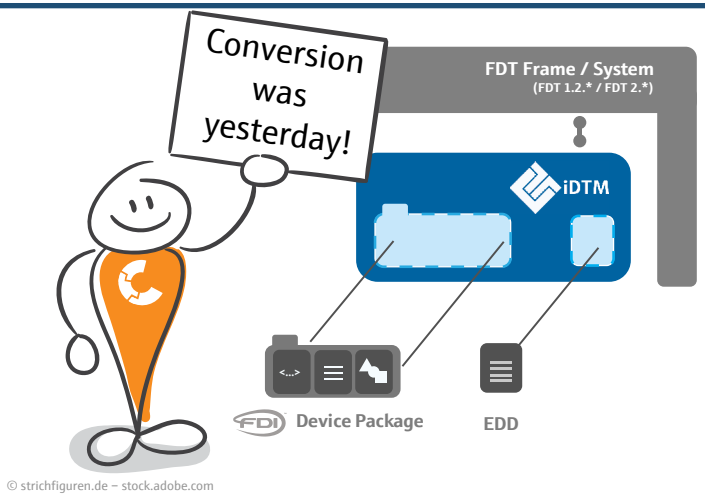
The FDT Server's X.509 certificate-based authentication schemes are tightly integrated with TLS to not only verify the correct server, but also confirm the client device is authorized to communicate with the server. This "triple handshake" of server, client device, and end-user authentication ensures that no impersonations, man in the middle attacks or otherwise unauthorized access is permitted. The use of encryption throughout the communication architecture ensures that no one can eavesdrop on any of the communications.

The various industrial control network organizations are moving towards a more robust security model for their respective protocols. One such example of security-on-the-wire is the newly released Common Industrial Protocol (CIP) Security Volume 8 by the ODVA organization. CIP Security coupled with FITS enables a complete solution for comprehensive, end-to-end, enterprise-wide security. The FDT Server will natively support CIP Security, linking the IT and OT security architecture with control. Security-on-the-wire will enable the control system to defend itself from unauthorized and/or malicious access. For instance, the layered approach within CIP secure EtherNet/IP™ allows users to implement EtherNet/IP with all control communications on the strongly authenticated, and optionally encrypted communications, to avert potential disruptions.

Finally, the FDT Server-based architecture can be deployed in the public or corporate cloud, allowing full replication of the server environment for instant cutover in the event of a virtual server or network failure. This improves availability, as all communications between a remote server and local control networks is conducted through a robust Virtual Private Network (VPN) tunnel or equivalent solution in order to obstruct intrusion attempts. The VPN establishes a secure connection from the cloud to an individual plant or factory while allowing redundant paths in the event of a cloud failure. It ensures that all communications between the remote FDT server and the physical plant(s) are carried in a hardened, encrypted VPN tunnel.

Integrating OPC UA Technology

A critical feature of FITS is the integration of an OPC UA Server providing the information model for enterprise level data exchange. Unlike patchwork solutions that try to gain access to some device information through OPC UA, the scalable FITS architecture natively employs an OPC UA Server allowing all devices on all networks to be accessed through the FDT Server. This capability requires no special configuration by the end-user. Any OPC UA Client that has the correct security profile can browse the entire plant project structure and access any information available from the FDT Server.



Directly use whatever is available to manage your devices with your FDT Frame Application - the last evolutionary step.

With iDTM **end users decide** which FDI Device Package or EDD to use directly in any existing FDT Frame (FDT1.2.x and FDT2.x). Device manufacturers are **not forced to deliver FDT/DTMs** to their end users. FDI Device Packages or EDDs that are available are sufficient and can now be used in all FDT Frames.

So why iDTM? Here are some aspects to be considered:

- Configuration, monitoring, troubleshooting of all devices with a single DTM
- No more search for device drivers
- Reuse existing EDDs or FDI Packages in iDTM-EDD and iDTM-FDI
- Wireless HART and APL support

Supported protocols:

HART COMMUNICATION PROTOCOL · FOUNDATION · PROFIBUS · PROFINET

Get your version now on www.codewrights.de

Now with PROFINET support! CodeWrights

Continued

FDT Solution Advances Industrial Cyber Security

All of the well-accepted security mechanisms prescribed by the OPC Foundation are supported for the certified OPC UA Server built into the FDT Server architecture. This includes:

Trusted Information (CIA Triad): The CIA Triad is a model designed to guide policies for IT security within an organization. The elements of the triad (confidentiality, integrity and availability) are considered the three most crucial components of security. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Access Control (AAA Framework): Access Control is the way organizations control access to the network server and what services are available to users once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which access control is set up on a router or access server.

FDT Group has taken a careful approach in developing the distributed FITS architecture to make sure that it correctly handles all the critical aspects of the CIA Triad related to data confidentiality, integrity and availability.

OPC UA

Conclusion

With growing reliance on connected systems in plants and factories, and ever-increasing amounts of data, it becomes more important for the ICS, its devices, and the data and points of connectivity to be inherently secure.

FDT Group's FITS platform has been engineered from the ground up to provide the assurance of utmost security with flexible deployment options for the process, hybrid and discrete markets. This solution will be optimized by continued review of best practice implementations backed by FDT's simplistic, secure-by-design approach.

Find Out How Endress+Hauser Makes Your Plant Intelligent

White paper focuses on mobilizing field device management in the era of connecting IoT with Field Xpert

Nicolas Mangold, Endress+Hauser

Endress+Hauser made the step of building the bridge between the plant's field and the enterprise intelligence on any level. With Endress+Hauser's new Field Xpert version 1.3 including the IIoT connectivity "Library", making a plant intelligent has become as easy as enabling your smartphone's cloud storage.

Endress+Hauser's Field Xpert is a PC/Tablet based universal device configuration tool that lets users perform mobile and intuitive asset management in hazardous and non-hazardous areas. It is suitable for commissioning and maintenance staff to manage field instruments with a digital communication interface and to record progress.

This tablet PC is designed as a complete solution that comes with pre-installed driver libraries.

It supports protocols such as HART, PROFIBUS DP/PA, FOUNDATION Fieldbus, Modbus, and Endress+Hauser service protocols (CDI, ISS, IPC and PCP).

Field Xpert incorporates the open FDT® technology standard and is compliant with FDT/DTMs. Many DTMs are included with the Field Xpert tool and get updated automatically. If any additional third party DTM is required, it can easily be integrated in few easy steps.

Key features:

- Fast single click connection to devices with smart hardware detection.
- Integrated Heartbeat Verification including PDF documentation
- Automatic file and document storage to their digital asset twins in "Library".

Continued

Find Out How Endress+Hauser Makes Your Plant Intelligent

Find out how Field Xpert smartly organizes your files when combined with Library.

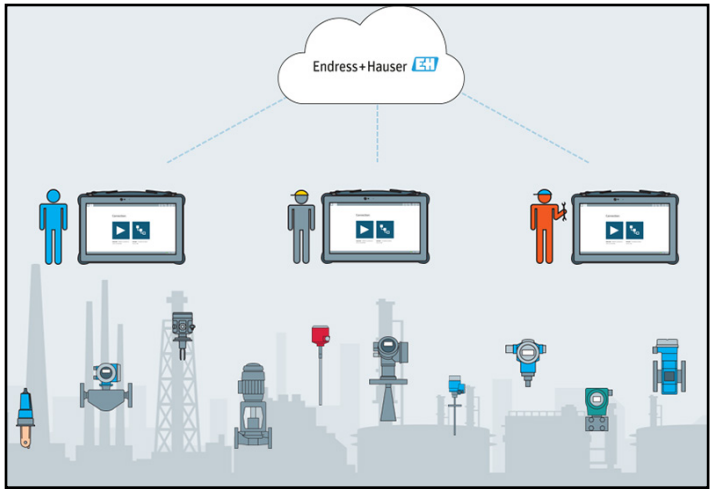
During the complete life cycle of a device, you generate plenty of files and documents that are relevant to your production and certification processes. The powerful Field Xpert add-on "Library" saves and organizes your working files and documents making everything safe, up to date and available everywhere at any time.

It is super easy. Like the iPhone works with iCloud, the only thing you need to do is connect your Field Xpert tablet with "Library" and it will start organizing all your working files and digital asset twins.

With its IIoT Eco-system, Endress+Hauser is showing how FDT standardized field device management tools easily empower the connected industry.

The Industry 4.0 is no longer the future. It is reality and it starts now with Field Xpert.

Find out how it works and how you too can make your plant intelligent, by downloading Endress+Hauser's "Smart device configuration management" solution.

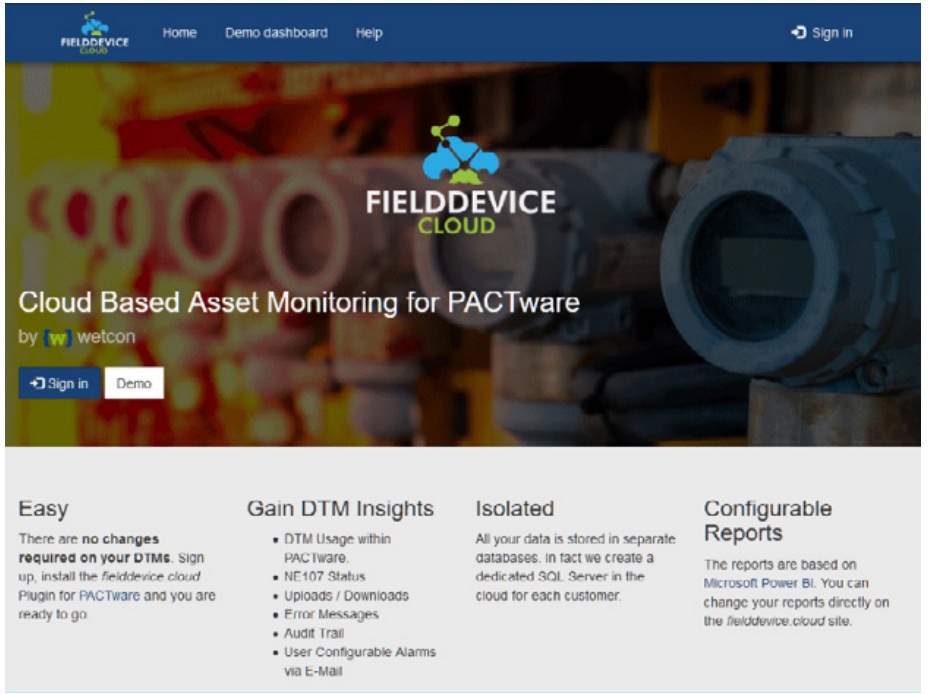


Fielddevice.cloud for PACTware

Cloud-based asset monitoring for field devices, out-of-the-box supported by PACTware

Mathias Hartner, wetcon

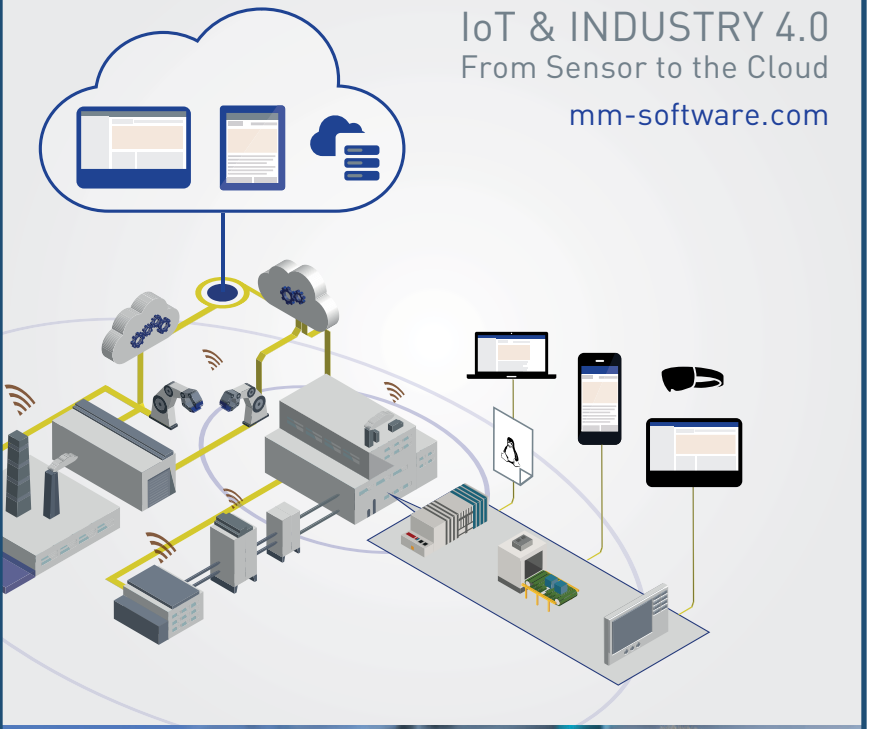
German company wetcon, with many years of expertise in device management solutions based on FDT and FDI, offers with fielddevice.cloud a cloud-based asset management for field devices as Software as a Service (SaaS). Thanks to a plug-in for PACTware, provided free of charge, this is available to all DTMs, hosted in PACTware, without them having to be modified.



The fielddevice.cloud web application provides statistical overview of configured device types, their geographic location information, editing users, NE107 status of devices, executed parameter up- and downloads, occurred error messages and parameter related audit trail information. This information can also be displayed for a dedicated device instance.

Within PACTware no additional user handling is necessary to provide this information to fielddevice.cloud. Instead, the plug-in takes over the logging of all activities and delivers the data to the field device service via a secure connection for the respective customer account. This works with all DTMs without any modification purely on the basis of the information provided via the FDT interfaces of a DTM.

The reports are highly interactive and based on Power BI from Microsoft. Power BI is a suite of business analytics tools, that delivers insights throughout an organization and is able to connect to a hundred of different data sources. Power BI based reports are highly interactive supporting any HTML5 based web browser. In addition, the reports can be modified directly by the fielddevice.cloud user within the web browser using an Excel oriented user interface. This can be used to provide additional information within a report, e. g. based on specific field device types.



Continued
Fielddevice.cloud for PACTware

The service is hosted in Microsoft Azure. This guarantees highest service availability and worldwide fast access times.

Within fielddevice.cloud, data of each customer is stored in separate databases, in fact fielddevice.cloud uses a dedicated SQL server in the cloud for each customer. A customer may also be able to access its monitored data using an ODATA service interface (on request).

Field device monitoring services may also be available for any other type of device or FDT/FRAME application. Source code for nearly any client can be generated automatically based on the OPENAPI interface of fielddevice.cloud REST services.

Usage of fielddevice.cloud is free of charge for 30 days. After that, payment is based on the number of connected field devices per day.

wetcon also offers a version via Microsoft Azure Marketplace, so that the fielddevice.cloud services and reports can be hosted within a customer owned Azure subscription. This would provide also the possibility to integrate other customer specific databases (e. g. production data and buyer information) into the Power BI reports.

For the connection of further field devices to fielddevice.cloud, wetcon offers appropriate support or realizes such an integration efficiently.

Additional information:

wetcon GmbH, 89250 Senden, Germany

www.wetcon.net www.fielddevice.cloud

support@fielddevice.cloud

Join the FDT Group

FDT Technology continues to be at the forefront of industrial automation advancement, with a truly open and standardized architecture to address the critical needs of the 'Connected World' of the Industrial Internet of Things (IIoT) and Industry 4.0. FDT Group has a strategic vision focused on the "Connected World" enabling a FDT/IIoT architecture supporting mobility, on-the-wire security, and comprehensive interoperability through an ecosystem of automation vendors providing tomorrow's new adaptive manufacturing assets.

Join other leading companies in the FDT Group today. There are unique advantages for the entire industrial automation industry – end users, suppliers/developers, service providers, universities, and individuals.

For membership information, please visit www.fdtgroup.org

FDT GROUP

FDT Group Members

ABB, APLISENS, auma, azbil, BACnet, Badger Meter, BARTEC, Baumer, BECKHOFF, Rexroth Bosch Group, bürkert, Chevron, CKD, CodeWrights, Danfoss, DET-TRONICS, Dräger, ELEMER, EMERSON, Endress+Hauser, FLEXIM, FLOWSERVE, HACH, hilscher, HMS, HollySys, BHsoftec, ITEI, KLAY-INSTRUMENTS, KROHNE, KUKA, M&M, Magnetrol, Maxonic, metso, MICROCYBER, MITSUBISHI ELECTRIC, NSD, OMRON, PEPPERL+FUCHS, PHOENIX CONTACT, ПОЛЮС, POWER-GENEX, Rockwell Automation, rotork, samson, Saudi Aramco, Schneider Electric, Shell Global Solutions, SICK, SIEMENS, SMC, softing, STAHL, SUPCON, TECHNISCHE UNIVERSITÄT DRESDEN, THORSIS, TOKY, TOKYO KEISO, TURCK, utthunga, Valmet, VEGA, WAGO, Weidmüller, WESTLOCK, wetcon, YOKOGAWA, YUDIAN, 宇通仪表

www.fdtgroup.org
FDT Group AISBL • 5 Industrieweg • 3001 Heverlee • Belgium
Phone: +32 (0)10 22 22 51 - Email: businessoffice@fdtgroup.org

February 2019 Issue