INDUSTRIAL AUTOMATION

IPP&T
INDUSTRIAL PROCESS PRODUCTS & TECHNOLOGY

CANADA'S PROCESS NETWORK

The automation of the industrial sector is about quickly and easily adapting manufacturing capabilities to where they're needed, based on ever-shifting market demands.

Industry 4.0 and the Industrial Internet of Things (IIoT) are integral components to reaching this goal within the new industrial landscape – but the unique demands of industrial automation are not easily solved with commercial IoT solutions.

The "industrial" in IIoT spans a wide range of solutions, including tools that simplify instrument maintenance, extended-life batteries that enable remote wireless devices, and much more.

Finding the right solution to your individual needs can be challenging, but it has been made simpler with these tools and techniques from some of industry's IoT leaders in this sponsored ebook from IPPT.ca.

INDUSTRIAL AUTOMATION IIoT 4.0

FALL 2019 VOLUME 1, NUMBER 1

PUBLISHER/AD SALES: Stephen Kranabetter
SKranabetter@ippt.ca

EDITOR: Don Horne
DHorne@ippt.ca

IPP&T INDUSTRIAL PROCESS PRODUCTS & TECHNOLOGY

CANADA'S PROCESS NETWORK

Produced By ANNEX BUSINESS MEDIA

SENSOR SURVIVAL IN RESISTANCE WELDING

WHAT TO DO ABOUT WELD SLAG

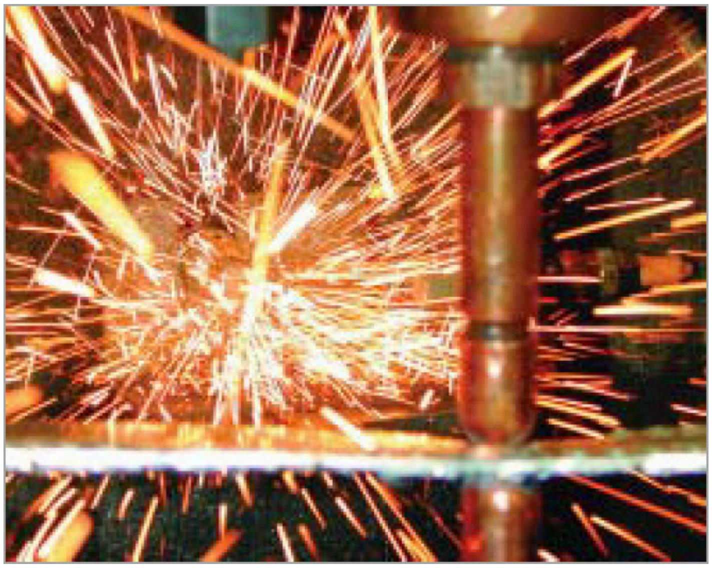
How often are sensors replaced in resistance welding applications? Imagine several sensors on several machines, all with a different degree of exposure to welding operations. This could be anywhere from a few sensors to a few hundred, depending on the application and industry. Also take into consideration where the sensor is in relation to the weld flash. Now imagine this: If a sensor fails in one operation and needs to be replaced it will cause a certain degree of downtime – maybe just a few minutes. But if another sensor down the line also fails and needs to be replaced, and so on down the line, this spirals into a productivity issue, not to mention a gross cost concern.

One of the most common applications where resistance welding occurs is in the automotive industry, where it is used to fuse parts of the car body. The welding temperatures are very high – often in excess of 1,200 degrees Fahrenheit – and currents can range from 15,000- 35,000 Amps. Sensors are used in this industry for multiple operations, including sensing where metal car parts are located to ensure proper placement prior to welding. An automated (robotic) weld arm maneuvers into place and welds in multiple locations around the vehicle. This causes sensors in proximity to the weld flash to experience different degrees of exposure and vulnerability to the effects of the weld flash.

Sensors are affected by the conditions resistance welding produces. Strong electromagnetic fields can cause a standard (ferrite core) proximity sensor to false trigger (output) or lock-on. Weld slag and/or splatter can accumulate on the sensor or melt the housing material causing small 'pock' holes to form. These areas are particularly vulnerable for further accumulation of weld slag/splatter. Depending on the sensor's construction (i.e. how well their material withstands weld by-products), it will withstand different levels of accumulation before malfunctioning. This is an obvious problem when position sensing is in use, and raises concerns for downtime, maintenance and associated costs.

Sensors in severe welding environments can fail (false output) as much as three to four times a day depending on the amount of welding involved in the application and where the sensor is located in relation to the weld tips. Sensors that are mounted very close to the weld tips are frequently subject to the weld flash, while those located further away will be affected by the flash, but not nearly to the degree to which those that are closer. For example, a sensor that is within 10 inches from weld tips can easily experience 1,000-2,000 flashes per day per switch.

To make a sensor with increased resistance to the weld flash, manufacturers have changed the sensors design to withstand varying degrees of weld slag/splatter. Some manufacturers use front caps made from Teflon, stainless steel or other materials, or use different materials for housing, like PTFE or copper. Some manufacturers use proprietary weld resistant material on the housing and/or front cap. It is generally more important to ensure the front cap is more resistant to the weld field, slag and splatter, while the housing can be less impervious to the slag/splatter and more resistant to the electromagnetic field. This is because the face of the sensor more often is directly exposed to the weld flash, and the slag/splatter will attach to the face but skid off the sides of the sensor with less likelihood of accumulation. Sensors that use stainless steel front caps are particularly prone to false outputs, as the oscillator must be tuned to the resonant frequency of the front face to sense through steel. Users commonly cope with sensor malfunction by simply replacing the sensor. Some are "repaired" using a tool (screwdriver) to chip off built up slag. A sensor that has been "fixed" this way will probably work for a period of time, but fail again and again by fewer weld flashes until rendered useless.



Some sensors designed for welding environments incorporate technology that makes the sensors resistant to the strong electromagnetic field. Factor one sensors that use separate, independent sender and receiver coils on a PCB and remove the ferrite core are inherently immune to the magnetic field interference that often occurs during electric welding operations, lifts and electronic furnaces. The absence of the ferrite core also allows factor one sensors to operate at a higher switching frequency.

Many sensors designated for welding applications by their manufacturers are not truly so, and fail after very few weld flashes. In fact, some sensors specially designed for weld resistance cannot function after 5,000 weld flashes. Sensors that can withstand 10,000-20,000 flashes are impressive on the low end and exceptional on the high end, though a select few can function beyond 20,000 weld flashes without failure. It is good to keep this in mind when choosing a sensor for welding environments to determine what level of resistance is best suited for your application.

To determine if your application would benefit from sensors specially designed for welding applications, you may consider auditing the rate at which sensors are expended in your current applications. How often are sensors failing? How often do you replace sensors? How much time does it take to diagnose or remedy the problem? The answers to these questions should help you determine how rugged a sensor you really need. Keep in mind that the effects of weld slag and splatter are not just harmful for sensors, but often affect surrounding components. Furthermore, sensors in these environments may be susceptible to human and mechanical damage. Some manufacturers incorporate fitted steel covers into the sensor housing prior to sealing the sensor so it's not a separate part – making the sensor impervious to physical damage from the side and weld damage from the front (when used with weld resistance front caps or coatings). In any sensing situation, it is important to examine all aspects that contribute to the success or failure of your sensors to make an informed decision regarding which sensor is right for your application.

CONNECTION COMPONENTS

Weld slag can also significantly affect the cordsets used to connect the sensors to higher level control systems in these locations. Weld slag build up is generally most harmful to the cordset where it mates with the sensor, or the quick disconnect area, if using a quick-disconnect sensor/cordset combination. If enough slag is present, it will effectively fuse the sensor to the cordset's coupling nut and require the cordset to be replaced along with the sensor. This may not sound like a big deal, but replacing the cordset can be very time consuming. Imagine removing 20 feet of tie wrapped cable – some of which is covered in solidified weld slag – and lying out, installing and tie-wrapping 20 feet of new cable.

There are ways to help avoid some of these cabling pitfalls. Depending on your application, you can choose from many different levels of protection. Cable jackets, plug bodies and coupling nuts are all components of the cordset that can be altered to provide weld slag protection. For instance, coupling nuts may be coated with PTFE to improve weld resistance.

Not just any cable jacket material can be used in these environments, as the slag will cause the cordset to melt or burn

on contact. Instead, cable jackets are made from materials that are more resistant to weld slag build up. The cable jacket most commonly used for welding environments is rubber (chlorinated polyethylene, CPE) for its ruggedness and durability. A thermo-set CPE jacket over EPDM rubber insulation is impervious to flame and temperature extremes. CPE jackets also provide superior resistance to tears, cuts and abrasions. The drawback of this cable type is that it is more difficult to strip and is not recyclable.

If the welding environment doesn't require cable as rugged as CPE, thermoplastic elastomer (TPE) jacket material may also be used. TPE cable, sometimes called TPR (thermoplastic rubber), provides very good resistance to weld slag build up. It is also more flexible, less expensive than rubber, and easier to strip. TPE material may also be used as molding for the cordset plug body.

If specifying different material is not enough to protect your cordsets, there are other options to further a cordset's resistance to these extreme conditions. If the weld slag is so extreme that the coupling nut is fusing to the sensor, adding a protective sleeve over the cordset should be the first option you consider. The sleeve, often made from fiberglass, fits over the cordset and the coupling nut to where it meets the sensor to protect it from weld slag. The sleeve is usually coated with another substance so it is better able to withstand the brunt of the damage from the weld slag. Sleeves can be made to fit most cordsets in lengths that are specific to the application. A second protection measure involves an expandable silicone rubber coated fiberglass sleeve. This method of provides a 'heat shrink' type fit around the cordset and the coupling nut.

Another option is to use a short extension cordset between the sensor and the second, longer cordset. Since most of the slag damage occurs near the sensor, adding the extension cordset, also called a sacrificial or shorty, to this area means you'll only have to replace the extension cordset and you won't have to go through the hassle of replacing a 20 foot cable.

DIGITAL PNEUMATICS

– early wins for Process Automation

Digitalizing pneumatics with the revolutionary Festo Motion Terminal (VTEM) opens up new opportunities to improve competitiveness in Process Automation.

With VTEM's digitally-controlled pneumatics, the days when a valve has only one function are over; the same ones can be used as both proportional or control valves. The valve terminal is then just like a reprogrammable piece of hardware and can even be reconfigured remotely. VTEM's 10 (and soon 11) Motion Apps define the functions of its piezo-based valve technology, and in so doing replace over 50 on-board components, from flow control valves to a wide range of directional control valves, proportional regulators, as well as hardware used for functions like soft stop and positioning. That represents cost savings in procurement, commissioning and maintenance, but it's in its ability to improve operational efficiency that VTEM truly shines for Process Automation.

Here are three examples of gains that can be captured by VTEM today:

1. Flexibility and precision: Presetting travel times.

In some industries, the working stroke must be precise and consistent; the stroke determines how long a valve is to be open. For example, with pharmaceuticals or cosmetics, it is essential to neither overfill or underfill containers. By presetting the travel time with the VTEM app, it is possible to specify exactly how much time the valve requires for switching. The app not only presets travel time, but also monitors performance, so if the switching time degrades due to wear on components, the app automatically adjusts to maintain the precise duration required. Also, presetting of travel time allows production lines to be reconfigured quickly. Rapid changeovers can be done in minutes for huge time and labour savings.

2. Reduced compressed air consumption: the ECO drive

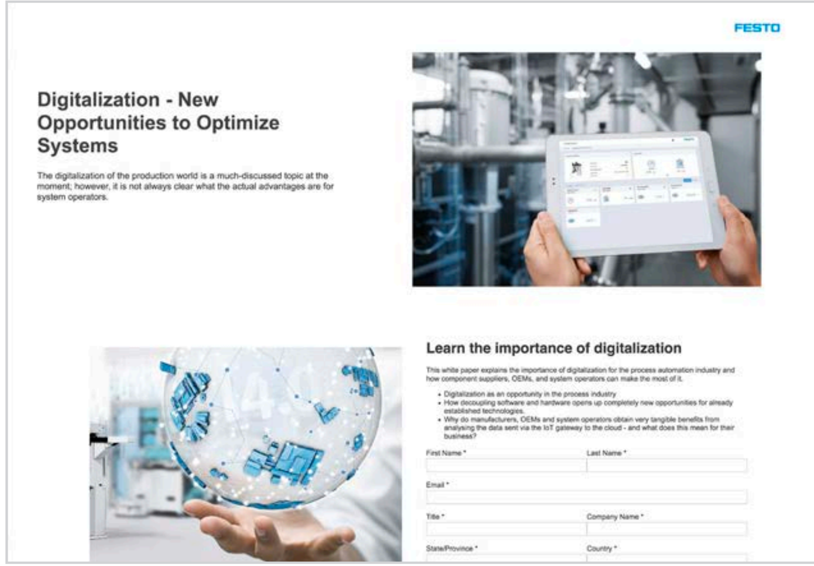
In conventional pneumatics, every actuator must be sized to provide more torque or force than required for the working stroke. It's a necessary safety buffer; for example, where only 300 Nm torque is required, a 450 kN actuator is selected to have sufficient reserves for production. This translates into higher compressed air consumption for systems in continuous operation. VTEM's "ECO drive" motion app is able to pare down compressed air consumption without compromising safety or production efficiency. Experience has shown that energy savings of up to 70 per cent can be achieved.

3. Leakage diagnostics

Air leakage is not something you have to tolerate but identifying leaks can be time-consuming and can only be done when the system is down. This is where the VTEM's app for leakage diagnostics helps. Faults are detected rapidly, and as the leaks can be actuator-related, pinpointed precisely. The app is testing continuously and can locate leaks at an early stage. The overall effect: this does away with the need for time-consuming troubleshooting vast pneumatic networks, and helps to reduce energy costs resulting from leaks.

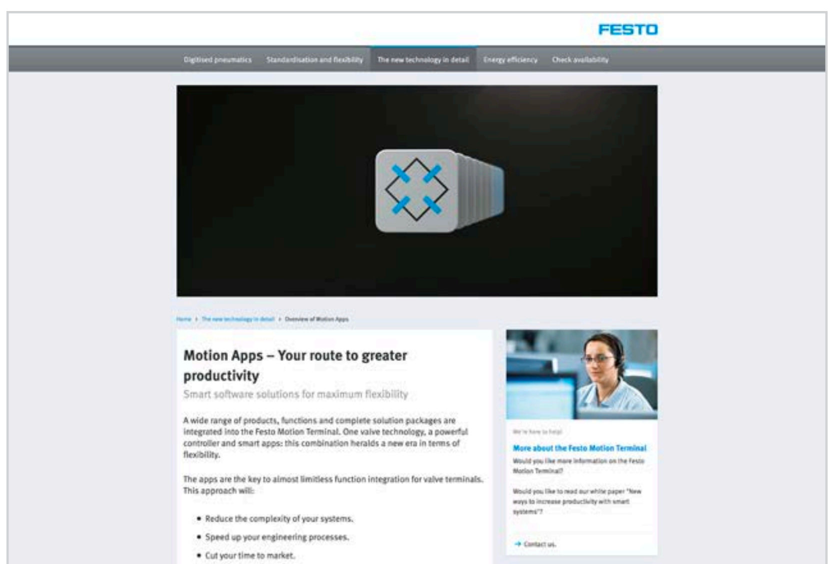
These are just some of the ways digital pneumatics with the Festo Motion Terminal is game-changing technology. The available apps support energy efficiency by reducing compressed air consumption and minimizing leakage. On the other hand, it has the flexibility to be used in production processes, saving commissioning and changeover costs – and its monitoring functions are automated and decentralized (localized to each valve).

Contact Information:
Festo Inc.
festo.canada@festo.com
www.festo.ca



To download our VTEM Whitepaper for Process Automation, **click here.**

For more information on the Festo Motion Terminal, **click here**



For more information on all available VTEM apps and their benefits, **click here.**

ESTABLISHING AN OPEN, MODULAR AND HOLISTIC AUTOMATION ARCHITECTURE

In order to compete and win in a global, competitive, fast moving world with increasing demands, all kinds of technology must be harnessed and put to good use. But without an effective approach to enterprise integration, all these technologies remain in silos and won't be useful to the business.

Technology collaboration between two leading open, automation industry standards organizations is changing the paradigm for integrating control systems, applications and devices within a unified architecture – all aimed at optimizing information exchange throughout the industrial enterprise.

Background

As two leading open, industrial automation standards organizations, FDT Group and OPC Foundation are working together to provide greater access to critical information throughout the industrial enterprise. FDT is the established integration standard, globally adopted with hundreds of thousands of FDT/FRAME™-enabled control and asset management systems and tens of millions of FDT/DTM™-enabled field devices, while the OPC Unified Architecture (UA) provides an infrastructure to make enterprise information available to thousands of other applications and platforms.

The FDT standard intersects the variety of networks attached to intelligent instrumentation and the higher-level systems that interact with these devices. It establishes an open, modular and holistic automation architecture that adapts to the changing requirements of suppliers and end-users. FDT incorporates a plant hierarchy based on a physical network topology coupled with a logical topology. The technology supports all the major networks employed in process, hybrid and discrete automation, and is adaptive to future networks as the industry demands. This approach makes it possible for FDT-based systems to transparently tunnel through disparate networks to gain access, and talk with any end device.

OPC UA, on the other hand, is focused on providing complete information modeling that allows industry stakeholders to take advantage of a service-oriented architecture enabling previously disconnected devices and applications to work together in a seamless manner. For example, OPC UA enables client applications to connect to server applications without understanding the syntax and semantics of the data compiled into the client application. This approach is all about simple discovery of the capabilities of the server, and efficiently leveraging its services and data.

Meeting today's data challenges

In November 2016, FDT Group and OPC Foundation announced the release of an FDT for OPC UA companion specification/annex for information modeling. This was an important milestone for standard integration of information provided by FDT/DTMs into the OPC UA information model.

Recently, the FDT Group worked with OPC Foundation to enable native integration that's supported both by OPC UA and FDT 2.x technologies. Instead of writing this integration capability into the FDT specification, the two organizations collaborated on a companion specification describing how to implement an OPC UA Server in an FDT/FRAME as part of the emerging FDT IIoT Server™ (FITS™) architecture. Most of the companion specification is devoted to outlining the data mapping between the two sides.

The FITS solution takes advantage of the FDT for OPC UA companion specification in enabling sensor-to-cloud, enterprise-wide connectivity for industrial control systems. It combines native OPC UA integration, web services and rich control network interoperability to optimize connectivity and information exchange for the next generation of automation. The solution also features robust layered security addressing all components of the server architecture.

Progress on information integration

Standard integration of information provided by FDT/DTMs into the OPC UA information model is essential for device diagnostics, configuration and remote asset management, as well for integration with higher-level business applications. This document defines an OPC UA Information model to represent the FDT architectural models. This allows an FDT/FRAME or FDT IIoT Server to expose project structure and device specific information through standard OPC UA mechanisms. While this mapping is an essential activity to achieve interoperability, it is completely transparent to the end user.

As part of the integrated FDT/OPC UA solution, the built-in OPC UA Server can read and write device information. Any OPC UA Client can access the FDT/OPC UA Server and obtain data as long as it has the right credentials. There are a multitude of possible clients within this architecture.

From the FDT standpoint, the aforementioned approach exposes its project tree to the OPC UA Client so that it can see what devices are accessible. As users click on each device, they can view and access its specific attributes and information.

OPC UA provides a uniform information exchange methodology between applications, whereas FDT provides network/device configuration and access to devices. The combined FDT/OPC UA approach enables unification of system engineering, configuration and diagnosis in Industrie 4.0.

The capabilities for OPC UA integration were introduced with the FDT 2.0 specification. Additional enhancements were made with the subsequent 2.1 version and will be strengthened in the 2.5 standard (also known as FITS), which is set to deploy in the 4th quarter of 2018.

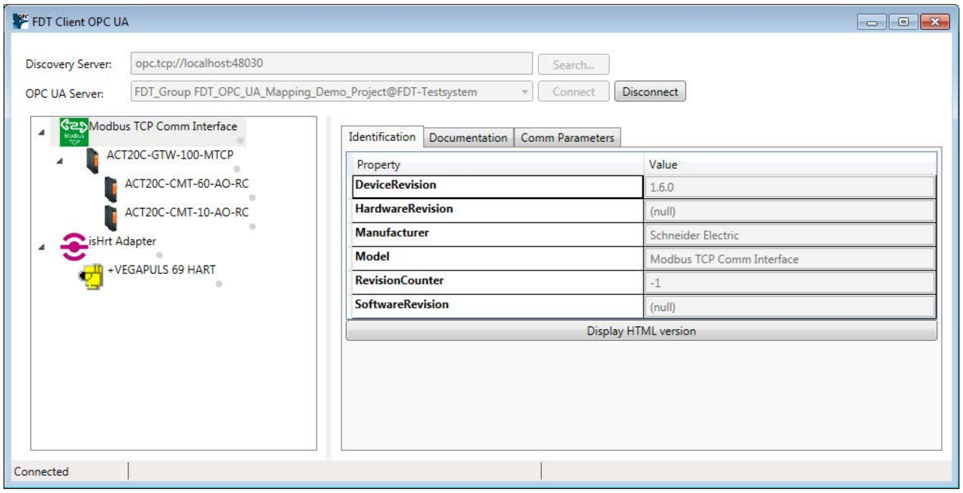


Figure 1: Screenshot of FDT OPC UA Client showing the project tree exposing what devices are accessible.

Optimizing network communication

We all know that process control and discrete automation systems, field devices and other electronic instruments are networked so they can exchange information. But how does that information get where it's supposed to go?

Within a traditional client-server (i.e., request-response) communication model, a client computer or software requests data or services, and a server computer or software responds to the request by providing the data or service.

For example, when sending a spreadsheet to the printer, the spreadsheet program is the client. Its request for printer services goes to the print server, which responds to the request and allocates resources for printers on the network. The print server handles all the client requests for printing, making sure the spreadsheet and other pending print jobs are all completed in an orderly way.

A different way for systems and devices to communicate on a network is called publish-subscribe messaging (i.e., a form of asynchronous service-to-service communication). In this model, any message published to the network on a topic is immediately received by all of the subscribers to the topic. Clients that publish the data send it only when the data changes. Clients that subscribe to the data automatically receive it from the server, but again, only when it changes.

The publish-subscribe extension enables public subscriptions for larger numbers of devices. The client-server model has drawbacks in this case, as a large number of connections would have to be established, each client would need to provide memory for storing the connection information, and high processor load would be generated in the server for encoding the individual messages per established connection.

OPC Foundation recently announced the release of a publish-subscribe (aka, "PubSub") specification to make the OPC UA standard compatible with emerging IIoT applications. Its mission is to provide a mechanism for publishing server data to many clients. With OPC UA PubSub, applications do not directly exchange requests and responses. Instead, publishers send messages to a message-oriented middleware, without knowledge of what, if any, subscribers there may be. Similarly, subscribers express interest in specific types of data, and process messages that contain this data, without knowledge of what publishers there are.

Among other things, PubSub allows peer-to-peer communication between industrial controllers, and between controllers and human-machine interfaces (HMIs). The peers are not directly connected and do not even need to know about the existence of each other. It also allows things like asynchronous workflows and OPC UA Servers to stream data to applications hosted in the cloud.

Improving information exchange

Thanks to ongoing FDT/OPC collaboration, members of the industrial automation industry have a choice of methodologies for implementing a network communication model that suits their specific needs. Both client-server and publish-subscribe models are included in the FDT for OPC UA companion specification.

With the client-server approach, the client goes through OPC UA to access current data values but must keep asking to verify the information. This is done either through a program in the OPC UA Client or by having an individual do a manual "refresh."

Alternatively, the emerging FITS architecture can employ a publish-subscribe methodology allowing sensor, network and topology information to permeate the enterprise, including mobile devices, distributed control systems (DCSs), programmable logic controllers (PLCs), manufacturing execution systems (MESs), enterprise resource planning (ERP) systems, the cloud, IIoT and Industry 4.0.

The publish-subscribe methodology eliminates the burden of request-response communication. Clients essentially say, "I'm interested in a particular piece of data, so please tell me whenever it changes." Multiple clients can subscribe and receive notifications at once. The server will automatically notify all the subscribed clients when the specified information has changed according to the pre-defined parameters. This approach has been proven to save valuable system bandwidth.

A typical use case for the publish-subscribe communication model is employing OPC UA and an FDT/DTM to monitor device health. By requesting notification only on changes in device condition, system and network resources are freed from continually polling the device to ascertain its health.

One of the key advantages of the FDT architecture is OPC UA is an easy plug-in.

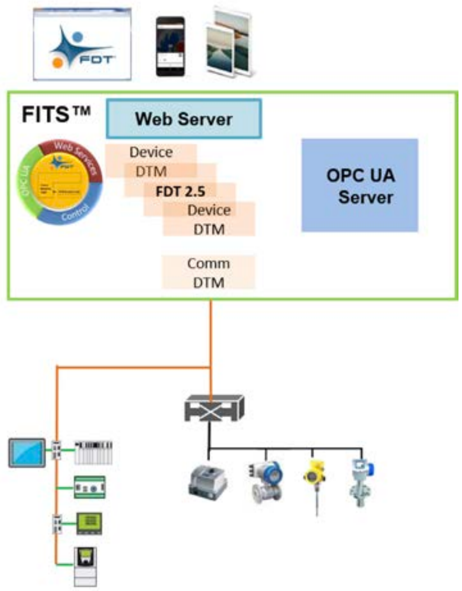


Figure 2: FDT IIoT Server (FITS) topology.

There's no need for changes to the communication, gateway or device DTMs. The FDT standard is robustly written so that it is only necessary to intercept communications at the right points within the FDT/FRAME or FDT Core Server in FITS to fully enable OPC UA. Plant or factory personnel can see all the networks on the server, as well as all FRAME applications and devices with DTMs through OPC UA. In addition, developers writing communication or device DTMs don't have any added requirements to support OPC UA. In the classic automation architecture, a DCS or PLC is located near the middle of the hierarchy and communicates with all of the upper level business systems like MES and ERP. This activity is completely eliminated with the integrated FDT/OPC UA solution.

Benefits to industrial enterprises

As described in this article, the FDT/OPC UA information model was designed to provide expanded integration capabilities along with ease of implementation. When industry stakeholders implement OPC UA, however, they may have challenges using the technology within their automation architecture due to the data trafficking role of the PLC or DCS. This could require the assistance of a process or control engineer to expose the required data from the control system to OPC UA.

FDT/OPC collaboration is intended to eliminate the typical constraints in industrial communication. When most engineers think of OPC UA, for example, they envision it running at the Ethernet level – but some kind of device hardware is needed to reach a compatible network. With the addition of FDT technology, users can take advantage of their existing infrastructure, thus bypassing any PLC or DCS that's in the architecture and communicating directly with end devices through OPC UA. As long as the device has a DTM in the FRAME or Server, the user will be able to access the device and all of its data through OPC UA.

If the user already has an FDT/OPC UA-enabled application in the architecture there is no need for additional configuration other than assigning security credentials. At that point, every bit of data inside FDT is accessible through OPC UA. Engineers are no longer faced with modifying ladder logic or writing rules for DCS systems. Thanks to an OPC UA Server inside an FDT application, all of the information is available. Nothing is held back, and there is no need for extensive configuration work to get the desired data. If a DTM is present, every bit of data about a device is available through the application.

Furthermore, IT departments utilizing MES or ERP systems don't have to consult with a PLC or DCS programmer every time they want to access specific types of control data. They can just browse the server structure and find the necessary information. IT personnel also have a choice of ways to interface with the FDT Core Server.

OPC UA is a known entity in the IT world with available tools to enable full connectivity and easy integration. As an option, FDT Web Services can be used to write Apps to support maintenance or engineering organizations. Users can access FITS through web sockets to browse project structures and perform other tasks.