DEVICE INTEGRATION STRATEGIES

Empowering the Intelligent Enterprise

CONTENTS

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.

FDT® GROUP

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

FITS™ Revolutionizes Next-generation Industrial Automation Strategies

FDT advancements realized with mobility prototype, member insight events: Developer seminars planned in 2018

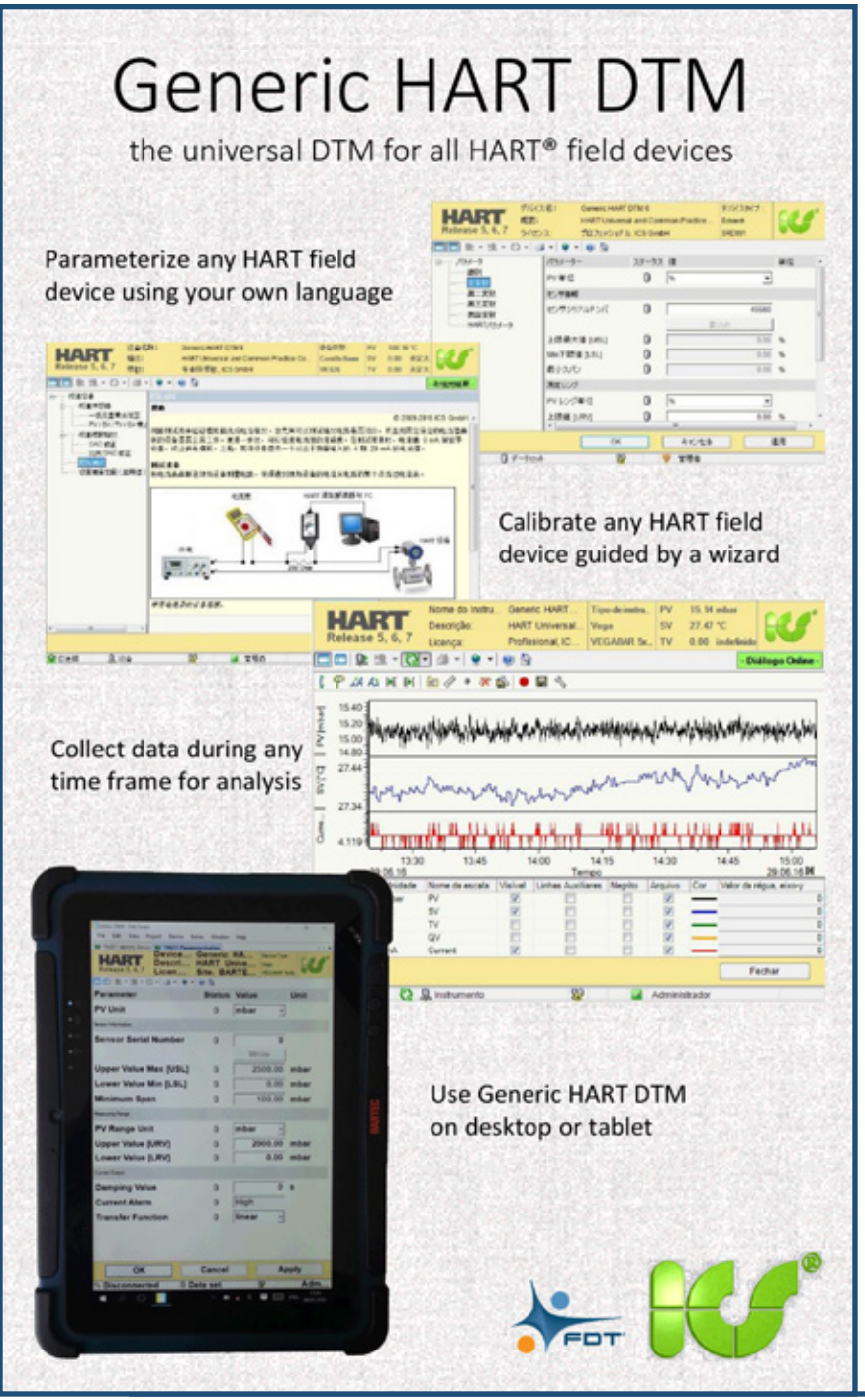
Lee Lane, Chairman of Board of Directors, FDT Group

We just concluded our first FITS developer seminar in Mannheim, Germany. This was a chance for FDT Group members to get a close-up look at the technology stack that drives our new FDT Industrial Internet of Things Server (FITS™) architecture. With more than 70 participants between the in-person attendees and those on the web, our member companies now have the critical information needed to properly place this emerging standard in their product roadmaps. It was great to see the enthusiasm for the architecture and the validation of the technologies chosen by our panel of experts. If you are an FDT Group member who couldn't attend the session, an on-demand version is available. Please contact our business office at businessoffice@fdtgroup.org for details.

Our next developer seminar for FDT Group members will take place in March, 2018. We plan to give members the opportunity to use the FITS common components to develop a working FITS DTM and install it on a cloud-based FITS server. Participants will also have the opportunity to create a FITS app, choosing an iOS, Android, or Microsoft platform, and connect the app to a FITS server in the cloud. An additional developer seminar will be scheduled near the end of 2018 when the final FITS standard is available.

A key component of our FITS architecture is the integrated OPC UA server capability, which was developed jointly with the OPC Foundation, who are continuing to refine its capabilities. I was pleased to see that a working demo of the OPC UA server component has been integrated in our tradeshow booth for the upcoming SPS/IPC/Drives trade fair in November. The native OPC UA capability within FDT has captured the attention of the user community as users seek to realize the intelligent enterprise envisioned in the IIoT and Industrie 4.0 initiatives. It is a powerful

FDT & OPC UA On-Demand Webinar: Empower a Single Approach to Enterprise Integration



Continued

FITS™ Revolutionizes Next-generation Industrial Automation Strategies

testament to the extensibility of FDT DTMs that this capability can be added without requiring any changes to the DTM that is supplying the information.

As we wind down 2017 and look forward to 2018, I would like to pause to thank the hundreds of volunteers that make the FDT Group what it is. Through the services of these member volunteers, we have completed nearly every objective that we set out for 2017. Our branding has been completely refreshed, a new website has been launched, brochures refreshed and translated, and our tradeshow/conference schedule has been expanded. We completed and approved new communication annexes, the FDT 2.1 standard, and we updated our certification tools. Our work on the new FITS architecture met its objectives and timelines. It is truly a pleasure to see the enthusiasm of the FDT Group members yield such tangible results.

ICS Built-in Security in Today's Connected Enterprise

ODVA, FDT Group cooperate on standards, tools that protect a connected company's assets. Joint development builds security infrastructure.

By Glenn Schulz & Katherine Voss

Over the last decade, the rise in cyber attacks on manufacturing facilities and critical infrastructure has resulted in cyber security becoming a central concern amongst industrial automation and control system users and vendors.

With the convergence of information technology (IT) and operational technology (OT) in industrial manufacturing, there is a need to safeguard data access from the enterprise all the way down to the device level.

The following article, by Glenn Schulz of FDT Group and Katherine Voss of ODVA, describes efforts by the automation industry to develop next generation standards and technology, which enhance security throughout the lifecycle of industrial control devices in today's connected world.

Introduction

As factory and plant operations become more connected in the era of the Industrial Internet of Things (IIoT) and Industrie 4.0, industrial organizations are making significant security investments to help protect their intellectual property, operations, and corporate image.

In the past, industrial control networks were primarily isolated systems, running proprietary protocols, using specialized hardware and software. But the industrial architecture has transformed over time, with

Figure 1: CIP Security™ is designed to protect Industrial Control Systems (ICS) in the new era of automation.

collaborative mechanisms that involve internal and external integration.

Industrial facilities have traditionally relied on logical or physical security to protect their perimeter. These defenses range from firewalls to gates, guards and fences. However, any breach in perimeter security can put the facility's industrial control system (ICS) at serious risk of denial-of-service (DoS) attacks or other disruptions.

Many plant sites employ a defense-in-depth security architecture to secure their ICS. This strategy is based on the idea that multiple layers of security are more resilient to attack. The expectation is that any one layer could be compromised at some point in time while the automation devices at the innermost layer would remain secure.

However, as attackers become more sophisticated, it becomes more important for the connected end device — the final layer of defense — to defend itself.

Evolving Security Challenges

Industrial security presents a difficult challenge in the age of open systems, increased connectivity and expanded data sharing. The fourth industrial revolution brings new cyber risks for plant and factory automation platforms. It is imperative for cyber security strategies to be secure, vigilant and resilient, as well as fully integrated into flexible business models.

As cyberspace shrinks due to the benefits derived from greater data exchange, new vulnerabilities in the ICS arise and new threats emerge. Left unchecked, the ICS, its devices and the networks to which they are connected, can be exploited by threat actors and pose potentially negative impacts on the safe, reliable and/or secure operation of production processes.

Governments and the private sector alike have expressed concern about cyber security vulnerabilities within automation systems. Regulatory bodies have identified threats to critical infrastructure where industrial Ethernet networks, such as EtherNet/IP, are commonly used. From a business standpoint, industrial firms are facing growing challenges from ransomware and other cyber threats.

With increasing reliance on connected systems, and ever-increasing amounts of data, it becomes more important for the systems, their devices, the data and points of connectivity to be inherently secure. Manufacturing plants have to give serious consideration to policies dictating how sensors and other edge devices can be accessed from the outside world.

One of the biggest concerns for end users is the industrial equipment lifecycle, particularly as it relates to the protection of data and access to crucial instruments. They must find ways to effectively address cyber security demands and protect plant assets such as field instruments, sensors and input/output (I/O) devices. A key issue is managing access to devices and their digitized artifacts over the entire lifecycle in a secure and reliable way.

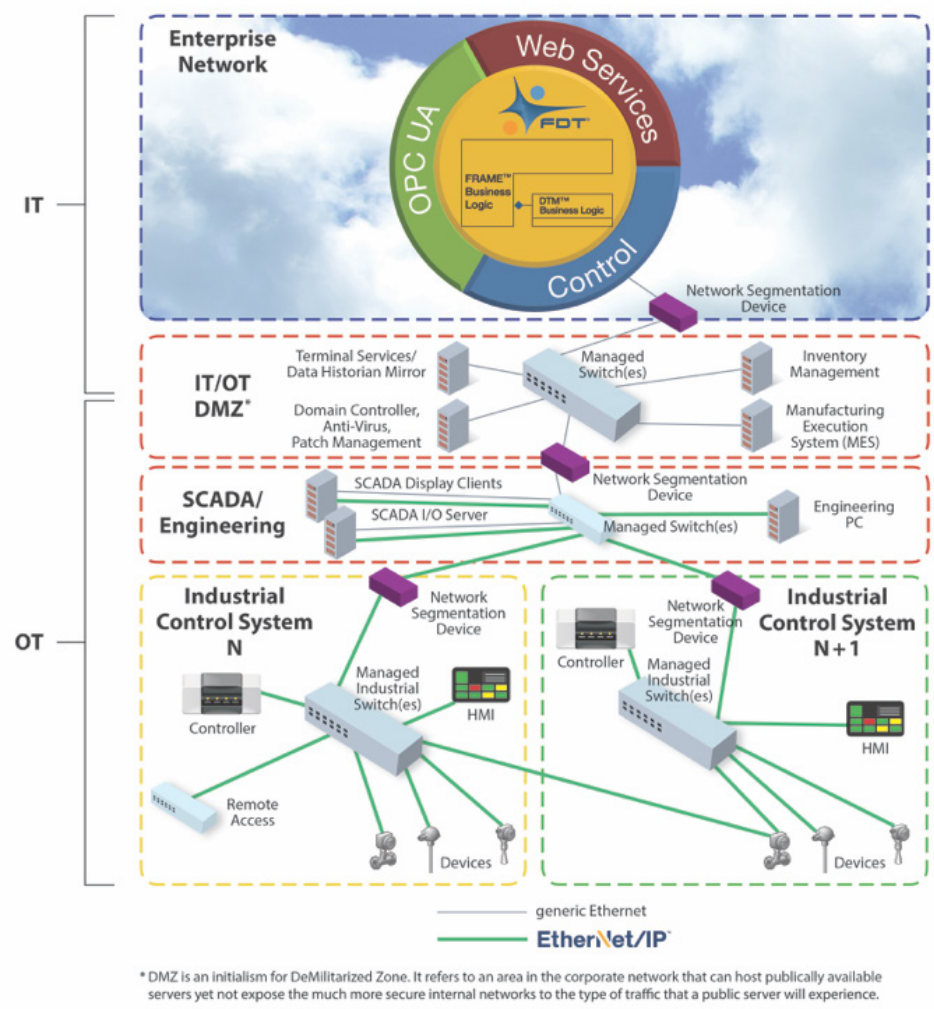


Figure 2: Converged IT/OT cyber security solution for the industrial enterprise

Advancing Industry Standards

International standards bodies concerned about disruptive and dangerous cyber security attacks on plants and critical infrastructure operations have already established guidelines, standards and policies to help mitigate risks of cyber security threats to industry. In addition, governmental agencies such as ICS-CERT with the US Department of Homeland Security are working with industrial enterprises to identify threats.

ODVA, a global standards development and trade organization, develops and maintains the Common Industrial Protocol (CIP), an open communication protocol designed for automation and data use cases in industrial control systems and used by EtherNet/IP, the world's largest industrial Ethernet network, and found in devices across diverse segments of the automation market.

CIP Security, first released by ODVA in 2015, allows users to take additional steps to protect their ICS with techniques for securing transport of messages between EtherNet/IP devices and systems, and thus reduce their exposure to cyber security threats. The goal of CIP Security is to enable the EtherNet/IP device to protect itself from malicious communications. ODVA's roadmap for CIP Security call for capabilities to be released in phases as shown in Figure 1. The first phase of CIP Security provides mechanisms to encrypt the transport of messages between EtherNet/IP ports and for certificates. In addition, recognizing that every EtherNet/IP device and system does not need to provide the same level of support for all defined security

features, CIP Security defines a Security Profile to allow for a scalable solution. A Security Profile is a set of well-defined capabilities to facilitate device interoperability and end user selection of devices with the appropriate security capability. In the next phase of CIP Security, capabilities will be added around role-based authentication and authorization and enhanced encryption methods.

On the integration side of the automation industry, FDT Group is an international, non-profit corporation providing an open standard for enterprise-wide network and asset integration. The organization was founded for integration and lifecycle management of devices. Ongoing advancement of FDT technology is leveraging major developments like the IIoT and Industrie 4.0 to enable end users to realize the true potential of decentralization, interoperability, integration, as well as a unified view of all data and functions across process, factory and hybrid control applications.

FDT was built to support a comprehensive, open architecture for the connected world of industrial automation networks and assets. It supports the current installed base, and will adapt to future technologies and protocols. FDT/FRAMEs and Device Type Managers (DTMs) based on the current FDT specifications (FDT 2.0) are digitally signed, providing tamper-proof software delivery and non-repudiation. Granular DTM security with enhanced user rights is added to the security settings.

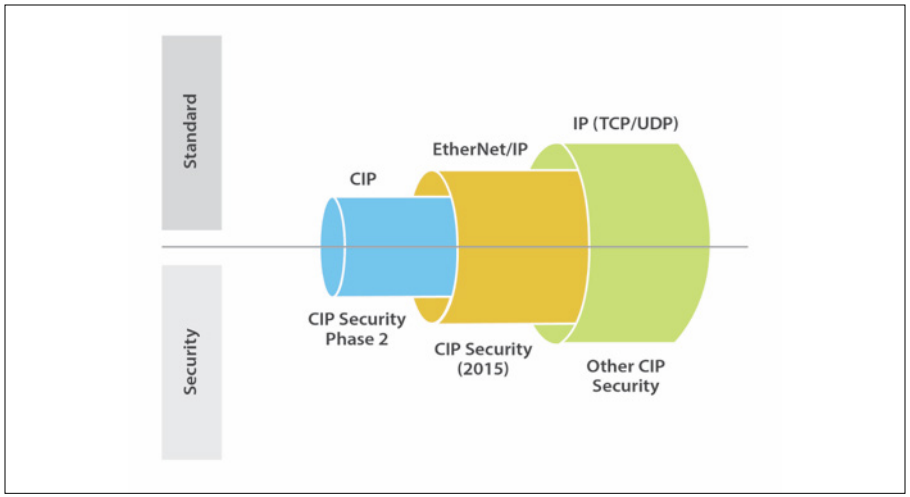


Figure 3: ODVA's Roadmap for CIP Security

Ongoing Industry Collaboration

ODVA and FDT Group are both working to address cyber security vulnerabilities with on-going enhancements to their technologies and standards. The two organizations have collaborated on the ability to integrate devices implementing ODVA technologies and standards into the FDT ecosystem for more than 10 years. The latest work resulted in a CIP annex supporting FDT 2.0, which allows for seamless tunnelling through industrial networks.

ODVA is one of the first standards development organisations to publish a true security overlay on an industrial network protocol. CIP Security utilizes standard encryption mechanisms and cryptographic

Continued
ICS Built-in Security in Today's Connected Enterprise

keys to provide scalable security on the wire. This approach is in response to recognition that every device in a production system is potentially a point of attack. With the growing use of EtherNet/IP within the ICS, there is a corresponding proliferation of malware into control networks and distributed assets.

As part of CIP Security, security on the wire will allow for end devices to defend themselves from unauthorized and/or malicious access — a critical capability with the move towards more connected systems. End users will have a choice of features they need to secure their particular environment. Because of the nature of typical workflows, devices will, in most cases, have CIP Security off by default and users will need to enable it. They will then have the option of more simple methods such as use of pre-shared keys for device authentication, or more sophisticated mechanisms like x.509 certificates. This will allow for the creation of a single zone of trust for devices, or multiple zones, depending on the application requirements.

FDT Group, at the same time, is focused on incorporating methodologies and workflows into its standard to support emerging security requirements. The organization is compiling a series of best practices to help manufacturers implement FDT solutions in a way that avoids possible threat vectors. In addition to an Audit Team to provide an independent perspective on security enhancements, it has established an Incident Response Committee to help ensure timely communication for active issues and provide a vision for long-term security activities, as well as a technical group within the Architecture and Specification Team responsible for a security framework for the development of new specifications and tools.

From FDT Group's perspective, any device that wants to communicate on

a control network must be part of an established security model. Devices such as I/O cards, transmitters, etc. need to have awareness of the network's security provisions and be able to participate in them. The same holds true for various software applications and tools.

To extend its support for the IIoT and Industrie 4.0, and simplify the automation ecosystem exchange, FDT Group is developing the FDT IIoT Server (FITS) solution. FITS enables mobility, cloud, and fog enterprise applications, as well as sensor-to-cloud and enterprise-wide connectivity employing FRAME and DTM business logic at the heart of its client-server architecture. The FITS solution features robust layered security, leverages vetted industry standards, and utilizes transport layer security (TLS) to establish a hardened shell and encrypt all communications throughout the architecture. Optionally, this solution can authorize devices that connect to the FITS server. User-based security is employed to determine the user's role and rights within the application.

The addition of security on the wire to the FDT standard will enable a complete solution for comprehensive, end-to-end, enterprise-wide security.

Forward-thinking Approach

As established international standards development organizations representing many of the world's leading suppliers of devices used in industrial control systems, ODVA and FDT Group have key roles in advancing end-to-end security for the connected enterprise, and in supporting the development of technologies and standards for security on the wire.

ODVA and FDT Group are committed to optimizing the industrial device lifecycle with robust built-in security features. Other potential collaboration between the two groups involves the security and authentication of tools and digitized artifacts within the FDT domain. This encompasses ODVA member suppliers utilizing DTMs in their field devices.

The next update to the CIP annex will embed CIP Security for seamless security integration and scalability of security control. In FITS, the FDT Server will natively support CIP Security to allow for security on the wire in a scalable format. It will link the IT and OT security architecture with control from the FDT/FRAME-enabled system. Security on the wire will enable the ICS to defend itself from unauthorized and/or malicious access.

When the ICS and its connected assets have inherent protection from cyber security threats, there is the possibility of access from other trusted systems that might otherwise be considered part of an untrusted IT system. Conversely, devices may be able to produce data that can flow more directly and securely to IT systems.

One issue for industrial organizations is that production systems, and the assets (devices) within those systems, have very long lifecycles. Some devices may allow for field updates with new security

Continued
ICS Built-in Security in Today's Connected Enterprise

capabilities. In other cases, the user would be looking at systems with varying degrees of device-level security. Tools such as firewalls or security proxies may be employed to help secure less-capable devices.

Ultimately, security on the wire will be implemented across the entire enterprise, from business systems down to the lowest device level. Any "open wire" will be regarded as a vulnerability and handled accordingly. As shown in Figure 2, technologies and standards, such as FITS and CIP Security, will provide users with a converged IT/OT cyber security solution for the industrial enterprise.

Conclusion

Industrial security is a complicated, multifaceted challenge that cannot be solved by simply purchasing the latest technology. Instead, managing the security of an industrial control network requires changing processes and managing risk.

ODVA and FDT Group share a similar vision for enhancements to ICS security technology. They recognize that is crucial to secure the control network itself in a changing cyber security environment. Indeed, every automation industry stakeholder must be aware of the crucial aspects of security throughout the lifecycle of industrial control devices in a connected enterprise ecosystem. Advancements such as control on the wire offer the opportunity for self-protected devices, which add another dimension of security to the industrial network hierarchy.

About the Authors

Glenn Schulz joined the FDT Group as Managing Director in July of 2009. Most recently, Mr. Schulz was the Managing Director and Vice President of Engineering at Dorner. For 13 years prior to that, he was executive at Rockwell Automation with responsibilities that included the Process Industry Asset Management businesses. Mr. Schulz was instrumental in establishing the legal, non-profit structure of the FDT Group that culminated with incorporation in Belgium as an AISBL. He holds international patents and patents pending in the area of industrial asset management and industrial network security, while also holding CISSP and ISSAP certifications with a focus in cryptography.

Katherine Voss is President and Executive Director of ODVA, Inc. The organization's technologies and standards include EtherNet/IP and the Common Industrial Protocol (CIP) among others Ms. Voss' career has included execution of business strategies and roadmaps for information and communication technologies (ICT) for the global industrial automation industry, as well as business model transformation for an international standards development and trade organization from a virtual organization to an international physical presence in North America, Western Europe and East Asia.

Securing Role-based Data Access Management for a Connected Enterprise

FDT2 makes it easier to set varying levels of security for different users, even altering user access when a plant's operating modes change.

Industrie 4.0 has sparked tremendous interest in connectivity, raising the possibility of enterprise-wide communications for industrial control systems. However, this complex, interconnected environment requires secure data access control management to protect against any attacks throughout the digital architecture, either accidentally or maliciously, causing severe damage upon personnel, equipment, infrastructure and the organization.

The FDT Group, an international, non-profit corporation providing an open standard for enterprise-wide network and asset integration, is supporting the new era of automation by making it easier to access information in plants and facilities with multi-generational assets that use one or multiple communication networks. The organization is also focused on incorporating methodologies and workflows into its standard based on emerging security requirements.

To meet the growing concerns of infrastructure security related to role-based management of critical information, FDT® (IEC 62453) plays a crucial part in access control and authentication. The technology was developed and designed with security measures in mind, and provides the vital building block methodology and infrastructure elements that address data access control to millions of facilities and plants empowered by FDT-enabled systems, supported by FDT

FRAME™ applications (FDT/FRAMEs™) and devices employing FDT Device Type Managers™ (FDT/DTMs™). Today, this installed base already reaps the benefits of role-based security features of DTMs that help provide security for human machine interfaces (HMIs).

In this article, we will specifically discuss role-based security management evolution within the FDT standard as it relates to the next-generation of automation supporting the Industrial Internet of Things (IIoT) and Industrie 4.0.

Role-based Control Management Evolves as Security Demands Increase

The FDT Group's legacy standard, FDT 1.2, released in 2001, includes provisions for role-based security for industrial automation systems and applications. It specifies a uniform user management model with predefined access rights for specific types of users. The standard identifies four user levels: planning engineer, maintenance engineer, operator and observer. Access control privileges for these various levels are determined by the DTM. Thus, specific sensitive functions of the FDT/DTM or the FDT/FRAME are only accessible to authorized users.

FDT technology provides clear guidance for DTM HMIs, and has continued to evolve to keep pace with market requirements for enhanced security features. However, there remains certain limitations in the context of field device parameters. FDT 1.2 normally doesn't provide functionality to configure parameter accessibility for different roles. For instance, an operator can configure LRV/URV for a given device using one DTM, but can't perform the same operation with another DTM without the required access approval. The access control permission is totally defined by the DTM. *Table 1* shows the example of this scenario.

The current FDT 2.0 standard, issued in 2012, incorporates bolstered security capabilities, including more granular DTM security with enhanced user rights and privileges added to the security settings. The predefined levels of security have been replaced with a user-defined capability, which allows industrial facilities to define who can have access to certain items – putting the level of security into the hands of the user.

Table 1 Parameter Access Control in FDT 1.2

DTM	Device	Parameters	FDT 1.2 User Roles			
			Planning Engineer	Maintenance Engineer	Operator	Observer
FDT 1.2 DTM A	Device X	Tag	RW	RW	RO	RO
		PV	RW	RO	RW	RO
		LRV / URV	RW	RO	RW	RO
FDT 1.2 DTM B	Device X	Tag	RW	RW	RO	RO
		PV	RW	RW	RW	RO
		LRV / URV	RW	RW	RO	RO

RW – Read/Write Access (Defined by DTM) *RO – Read Only Access (Defined by DTM)*

With FDT 2.0, user levels are simplified to three levels: engineer, observer and expert. Similar to FDT 1.2, the engineer has a full permission set and the observer has a reduced permission set. However, the expert category provides access control capabilities and functions that are enhanced by allowing system engineers to configure the accessibility of DTM functions and parameters using the FDT/FRAME application. This provides more control for the systems. FDT/DTMs may be integrated in different FRAMEs, which may have varying access requirements. They may restrict visibility and accessibility of devices and some data. Restrictions can be established to provide plant safety

Continued
Securing Role-based Data Access Management for a Connected Enterprise

or to present customized views for different users. The FRAME can easily be used to configure the desired access control settings for any expert. The privilege of the functions and data can be changed, depending on where the DTM is used or which operational phase is active. For instance, an expert user may have full control when the plant is being configured or upgraded, but changes to devices may be restricted when the plant is in production state.

Additionally, an expert may have different permissions for a single device and DTM when the device is connected in the plant or in the device lab. In the device lab, the user may have all the necessary authorizations to calibrate or commission the device. Minimal changes may be allowed when the instrument is connected later to the actual running control system.

In a nutshell, the privileges of data access and function invocation are configurable via the FRAME based on the plant operational state, individual user or team experience, and other factors. *Table 2* shows some example scenarios.

At the August 2017 FDT A&S Working Group meeting, there was a presentation of an access control prototype that proved the FDT 2.0 access control capabilities. The prototype also demonstrated that access control can be tailored according to specification needs. In the prototype, an engineer could easily set up and configure the expert's accessibility via the customized FDT/FRAME. Furthermore, the engineer could configure the role-dependent access rights of DTM HMIs.

Expert users could only operate on the functions or modify the parameters allowed by the engineer. In this case, FDT 2.0 provides flexibility to the user to configure parameter access rights. For instance, expert users can commission LRV/URV for Device X using DTM C or

Table 2 Parameter Access Control in FDT 2.0

DTM	Operation Phase	Device	Parameters	FDT2.0 User Roles		
				Engineer	Expert	Observer
FDT 2.0 DTM C	Engineer	Device X	Tag	RW	C (RW)	RO
			PV	RW	C (RO)	RO
			LRV / URV	RW	C (RW)	RO
FDT 2.0 DTM D	Production	Device X	Tag	RW	C (RO)	RO
			PV	RW	C (RW)	RO
			LRV / URV	RW	C (RW)	RO

RW – Read/Write Access (Defined by DTM) *RO – Read Only Access (Defined by DTM)*
C – Configurable (Defined by Engineer)

DTM D, as long as the right to access that parameter is granted by the engineer. *Table 2* illustrates an example of this scenario.

To summarize, the FDT Group is at the forefront of the new era of automation, supporting a comprehensive, open architecture for the connected world of industrial automation networks and assets. Ongoing advancement of FDT technology is leveraging major developments like the IIoT and Industrie 4.0 to enable end users to realize the true potential of decentralization, interoperability and integration. It is also providing robust, user-defined security capabilities that enable industrial sites to take control system security measures into their own hands.

The current version of FDT employs a standardized access control facility and infrastructure. With proper implementation by all vendors, FDT/DTMs can allow users to carry out a wide range of commissioned actions. Roles can be easily created, changed or discontinued as the needs of the plant or industry evolve. Data can be more securely protected by setting varying access levels for different user roles. Centralized administration can effectively reduce management cost. With these technologies, FDT has created a more connected, integrated and secure industry automation service, which can be very valuable to customers.

Authors: Jason Chan Sin Wai– member of FDT Group Architecture & Specification working group

Sham Wai Rock– member of the FDT OPC-UA project group.

FDT Technical Overview Brochure

This brochure provides an in-depth description of FDT; including an overview of the technology, historical development, practical applications of FDT in use and implementations, and so much more.

Click here to download the brochure

RemoteConnect Software Tool Cuts PAC Programming Setup Time

Schneider Electric's RemoteConnect, an all-in-one FDT 2.0 FRAME-enabled tool, supporting local or remote SCADAPack x70 management

Schneider Electric's new family of remote Programmable Automation Controllers (rPACs) can link local assets in widely-dispersed remote sites and the company's SCADA system, including valves, transmitters, sensors, etc.

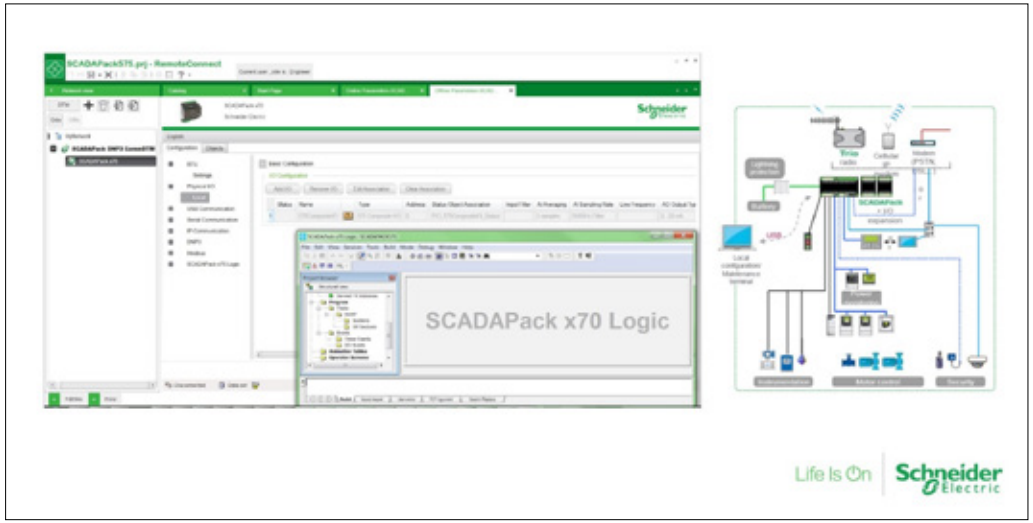
Made for the harsh conditions, the SCADAPack 570/575 rPACs transport field data through low bandwidth, unreliable or non-permanent communication links (cellular, PSTN, radio, etc.).

The family is configured and programmed using a new software tool, RemoteConnect, an FDT 2.0-based on FRAME that offers a logic editor window like Schneider's Unity Pro software.

RemoteConnect's main characteristics are:

- Open standard IEC 61131-3 programming environment
- Open standard telemetry protocols DNP3 level 4 with Secure Authentication and IEC 60870-5-101/-104
- Open standard industrial protocol Modbus RTU and MODBUS TCP
- Support of HART™ pass-thru to smart instruments and actuators
- Data concentrator for DNP3 and Modbus devices
- Multiple active SCADA masters, up to 200 remote/local slave devices and up to 90 remote peer devices
- Remote maintenance (ability to remotely perform configuration changes, program downloads, firmware update and diagnostics)
- 1ms resolution time-stamped digital inputs, 30ms sampled analog inputs
- 3 Ethernet and 4 Serial ports, 1 USB device port for configuration, 1 USB host port for external storage

Typical applications for rPACs include remote sites in oil & gas (upstream and midstream) as well as in water applications (irrigation, fresh water distribution, waste water collection, etc.).



Continued
RemoteConnect Software Tool Cuts PAC Programming Setup Time

RemoteConnect software is an all-in-one software tool used to configure and program the SCADAPack x70 range. This can be done either locally using any communication port or remotely through communication devices like serial modems, Ethernet routers or Serial/Ethernet radio units like Schneider Electric Trio™ Data Radios.

RemoteConnect software is built using Schneider Electric shared technologies such as industry standard FDT2/DTM and Modicon Unity logic engine (IEC 61131-3 logic programming). RemoteConnect software lets users manage SCADAPack x70 rPAC systems:

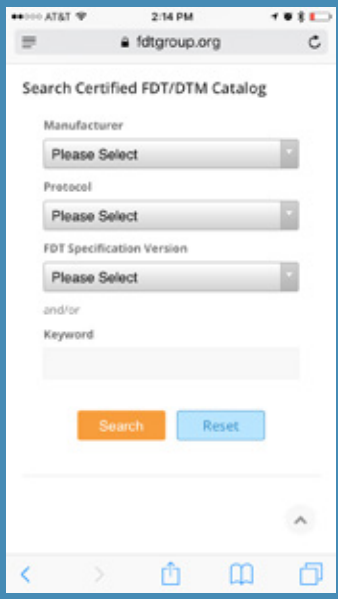
- create the rPAC configuration and logic file, offline
- download the rPAC configuration and logic file, locally or remotely
- upload the rPAC file including the logic program source for editing or debug, locally or remotely
- amend a configuration on the fly, locally or remotely through IP or non- IP communication links
- amend a logic program on the fly, locally or remotely
- perform rPAC diagnostics, locally or remotely
- update the rPAC firmware, locally or remotely
- export and import bulk configurations managed by spreadsheets or other applications
- manage external equipment using FDT 1.2 and FDT2 DTMs such as instrumentation, motor drives, etc. from inside the RemoteConnect environment

RemoteConnect software has an import/export command that enables a user to exchange relevant parts of logic programs with Schneider Electric Modicon M340 and M580 PACs.

- a program written with Schneider Electric Unity Pro for a Modicon M340 or M580 PAC can be imported by RemoteConnect software, compiled and loaded into a SCADAPack 570/575 rPAC.
- a program written with RemoteConnect software can be exported to Unity Pro, recompiled and loaded into a Modicon M340 or M580 PAC.

Click here to learn more about RemoteConnect.

Searching for FDT/DTMs™ Just Got Easier



FDT Group's website is the one-stop-shop if you're looking for certified DTMs™ for your intelligent devices. The upgraded product catalog features new filter & search capabilities and is mobile friendly!

FDT Group

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

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

November 2017 Issue