FieldComm Group™
Connecting the World of Process Automation

The **Value** of FDI

FDI Security

Visit **Ask4FDI.com** NOW for:

> All *The Value of FDI* articles

> Informative Videos

> Sample Bid Specifications

Abstract

In the era of digital transformation, with the growing convenience and use of the Internet, modern manufacturing systems must contend with new security risks. Safeguarding critical manufacturing assets require a holistic approach that deploys multiple layers of defense to address distinct types of threats.

This article covers the cyber security challenges faced by the process automation industry, security measures taken in FDI technology and the benefits that FDI brings in by mitigating such security threats for the end users.

The audience of this article includes instrument suppliers, system suppliers, cyber security professionals, automation engineers, business and technical leaders in the process industry.

Security Challenges in the Industry

Cyber security threats are intensifying every day, posing new challenges for security experts and additional barriers for connected plant operators. The ever-increasing connectivity is leaving the plant operators open and vulnerable to a multitude of unauthorized access attempts and data distortion. The device manufacturers must ensure security as a part of their product's lifecycle. Exploitation of software vulnerabilities such as Remote Code Execution (RCE), Denial of Service (DOS), remote access to process configuration etc. disrupt operations and cripple productivity of the plants. Detecting and eliminating these vulnerabilities is crucial for the safety of the plant and its assets.

FDI: A Secure Way to Interoperability

FDI technology deploys state-of-the-art security measures to mitigate possible threat vectors in the process industry. FDI enables system-wide integration of devices while providing additional capabilities and security. FDI security measures such as time stamping on Device Package signatures, sandbox environments for UIPs, and OPC UA security capabilities are explained below.

Secure FDI Package

An FDI Device Package is a sophisticated and standardized container for all the components that are required to describe a field device in the plant. An FDI Device Package should carry one or more digitally signed FDI Registration Certificate(s) to ensure its authenticity and integrity. FDI technology's security is enabled at multiple levels and undergoes rigorous testing and registration to ensure its safety from unauthorized access and tampering. Below is an outline of the testing and registration process.

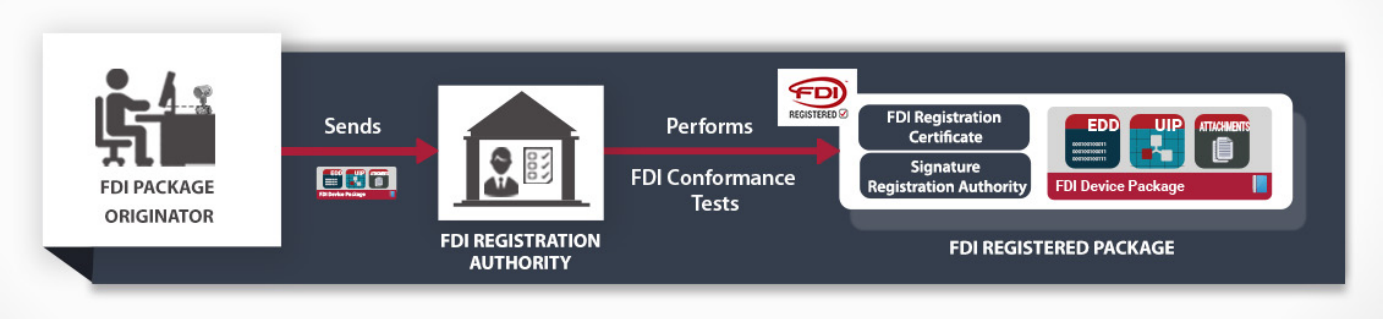
FDI Security

Create FDI Package

An **FDI Package Originator** (e.g. device supplier) creates an FDI Device Package as per the FDI specification, which contains the Device Description File (EDD), optional User Interface Plug-Ins (UIPs) and a set of documents/attachments related to the field device.

FDI Device Package Registration

The FDI Package Originator sends the FDI Device Package to the FDI Registration Authority (e.g. FieldComm Group) for registration. An **FDI Registration Authority** has the right and the ability to perform FDI conformance tests on the FDI Device Package. On successful completion of the conformance tests, FDI Registration Authority issues the **FDI Registration Certificate**, which is incorporated into the FDI Device Package as shown.



The FDI Registration Certificate may also contain information like what has been covered under the conformance tests.

Digital Signature on the registered FDI Device Package

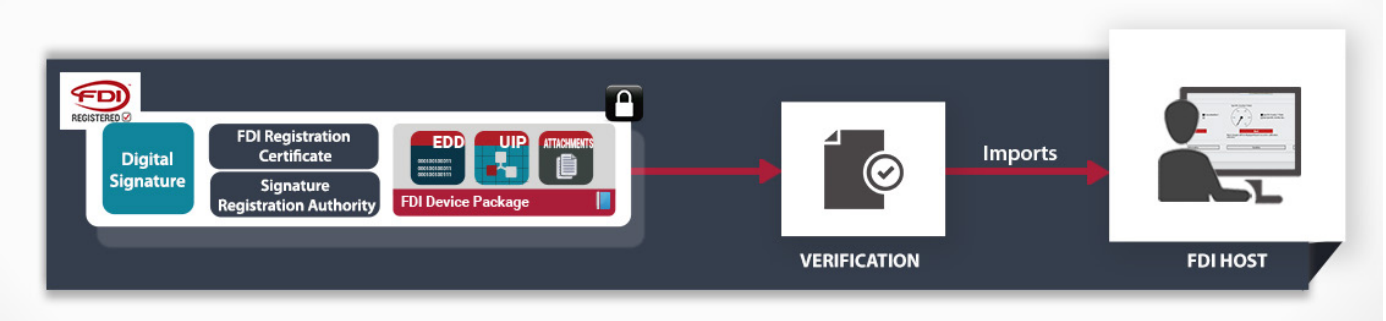
After successful registration of the FDI Device Package by the FDI Registration Authority, the FDI Package Originator again digitally signs the registered FDI Device Package. Therefore, FDI Package Originator takes the overall responsibility of the authenticity and integrity of the entire FDI Device Package and enclosed FDI Registration Certificate before its release to the end user.

During the digital signature procedure, the FDI Package Originator shall ensure that the algorithms used in creation of the digital signature shall be from the list of NIST recommended algorithms in FIPS 140-2 and shall include a trusted timestamp in compliance with XAdES (XML Advanced Electronic Signatures - ETSI EN 319 132-1). The certificate used for the digital signature shall be from the trusted Certificate Authority (CA) and it shall include the information required to validate the digital signature by the host system.

FDI Security

Verification by the FDI Host

During the FDI Device Package import procedure, FDI Host system will check the signature and certification status by reading the FDI Registration Certificate in the FDI Device Package. When the FDI Host recognizes that a digital signature on an FDI Device Package is not present, broken or not trustable, it shall display a warning message notifying the end user of the possible security threats. An FDI Host system shall specify which part of the FDI Device Package has been altered to provide better insight to the end user. Based on host-specific security requirements, a host system may allow a user to choose to import an FDI Device Package without an FDI Registration Certificate.



UIP Sandboxing

A User Interface Plug-In (UIP) is a software component in the FDI Device Package to represent complex device functionalities using rich Graphical User Interface. UIP is an executable element of an FDI Device Package that is executed by an FDI Host system. However, there is a possibility that a compromised UIP may contain malwares that access critical host system resources and possibly exploit host system vulnerabilities like remote code execution, file manipulation, data distortion etc. Hence, it is crucial for FDI Host systems to impose security measures during the execution of the UIPs.

In order to counter these security threats, FDI technology implements the **UIP Sandboxing** mechanism for executing UIPs. Sandboxing is not only a valuable tool for cyber security, but also for overall system integrity. UIP Sandboxing forces UIPs to run in a separate process with appropriate user credentials. Therefore, it isolates UIP execution to a tightly controlled set of resources in a system - thus mitigating security risks and system process overload.

OPC UA Security

OPC UA is the interoperability standard for the secure and reliable exchange of data in the industrial automation space. The objectives of OPC UA Security are authentication of client and server, authorization of user, integrity and confidentiality of data. OPC UA has been designed with built-in security mechanisms to address these complex security needs. In FDI, OPC UA acts as a secure communication channel between an FDI Server and an FDI Client, which can be either an operator station or HMI (Human Machine Interface) application.

End User Benefits

Reduced Security Threat

A multitude of field devices and host systems designed by various vendors co-exist in a plant. Seamless exchange of data in such a heterogeneous environment is vital for smooth plant operation. A standardized device integration technology plays a crucial role in the safety of that entire ecosystem.

When the field device gets integrated, the standardized device driver may act as a threat vector for malicious attacks on the host system. However, FDI technology has been designed keeping security in mind. FDI Device Packages undergo rigorous testing and are digitally signed to ensure their authenticity and integrity. FDI technology affirms that a UIP component within the FDI Device Package has controlled access to the system resources so that even the compromised UIP will have very limited adverse effect on the host system, thus reducing the security threats.

Reduced Maintenance Effort

An FDI Device Package is not an executable software and importing the FDI Device Package into the host system reduces the security risk. Moreover, the security patches made to the host system during maintenance do not affect the FDI Device Package. Multiple versions of same FDI Device Package can co-exist irrespective of the underlying operating system - thus reducing the risk and maintenance effort of the host system.

Conclusion

Amidst the ongoing digital transformation in industry, cyber security threats pose major challenges to Industrial IoT adoption. Cyber-attacks on infrastructure has raised concern on the safety of the plant and its assets – arguably to the benefit of the industry. Security has become top of mind and a key consideration during technology adoption. It is crucial for manufacturers to adopt new and robust methods of defense to mitigate emerging security risks and FDI technology aids in that endeavor.

FDI enabled products offer hassle-free integration of field devices into the control system. Stringent FDI Device Package registration process ensures the highest level of interoperability and safety of plant assets. The key features such as time stamping on FDI Device Package signatures and UIP Sandboxing mechanism affirm that FDI standard meets the stringent security needs of plant operators as they move forward in IIoT and Industrie 4.0.

FieldComm Group™
Connecting the World of Process Automation

FieldComm Group
9430 Research Blvd., Ste 1-120
Austin, TX 78759 USA
info@fieldcommgroup.org
+1 512.792.2300
www.fieldcommgroup.org