Basic background information on the development of the xDS concept

Todd A. Snide
Schneider Electric
Paul Brooks
Rockwell Automation
Dominique Leduc
Schneider Electric
Olivier Wolff
Endress+Hauser

Presented at the ODVA
2018 Industry Conference & 18th Annual Meeting
October 10, 2018
Stone Mountain, Georgia, USA

Abstract

As automation systems become more digitized and more modern, by taking advantage of advancing technologies, so must the support behind these systems. The EDS (Electronic Data Sheet) file was adopted by ODVA in the early 1990's and has been used since then as the device descriptor for CIP (Common Industrial Protocol) devices. The EDS file no longer meets the needs of modern automation systems. A device descriptor technology is needed for any automation system. ODVA has embarked on the development of a new device descriptor technology temporarily called the xDS concept. xDS concept will be more than just a device descriptor file. It will be technology concept to provide all the services performed by the EDS file and much more. This paper will provide the background information that is the basis for the xDS concept for CIP and will discuss some of the key features and support functions provided by the xDS concept. The xDS concept will be developed in ODVA under the SIG (Special Interest Group) structure in future.

This paper will discuss the background information to be provided to the new SIG. It is an introduction to the xDS concept with some of the primary needs, functions and tools to support the overall concept. As the xDS concept is officially developed within ODVA, the xDS concept may deviate from the scenarios described in this paper. However, the general application of the xDS concept can be understood from this paper.

Keywords

Digitization, digitalization, device integration, Industrie 4.0, digital twin, controls integration, edge/cloud integration

Definition of terms, acronyms and abbreviations

API	-	Application Program Interface
CIP	-	Common Industrial Protocol
CNC	-	Centralized Network Configurator
CUC	-	Central User Configurator
DoC	-	Declaration of Conformance
DTM	-	Device Type Manager
EDS	-	Electronic Data Sheet
FDI		Field Device Integration
FITS	-	FDT IIoT Server
I4.0	-	Industrie 4.0
IIoT	-	Industrial Internet of Things
IoT	-	Internet of Things
GSD	-	Generic Station Description
ODVA	-	standalone acronym
Pdf	-	Portable document format
RBAC	-	Role-based Access Control
SIG	-	Special Interest Group
STC	-	StatemenT of Conformity
TSN	-	Time Sensitive Network
URI	-	Uniform Resource Identifier
xDS	-	x(unnamed) Data Sheet (signed in the architectures)
xDS’	-	x(unnamed) Data Sheet’ (unsigned in the architectures)
YANG	-	Yet Another Next Generation

Introduction

As stated in the Abstract, the EDS file has been the staple artifact for ODVA for the purpose of a device description since the early 1990’s. The choice of the EDS file was state of the art at the time of its selection. However, a lot has changed since the 1990’s. The needs of automation systems have increased dramatically. The data created and consumed in an automation has grown and the value of data usage within and outside of the automation network has become well known. The Internet of Things has become a reality in industrial automation. The EDS file no longer functions well in automation and needs to be upgraded or replaced.

This leads to the development of a new artifact inside ODVA to perform the greater needs of modern device descriptor technology, the xDS concept. xDS is more than just a descriptor file and throughout this paper we will strive to explain xDS in greater terms than just as a device descriptor. Digitization is a common term used to describe the modernization of industrial automation systems. The xDS concept is part of the digitization effort for automation systems using CIP (EtherNet/IP, etc.) and related technology. It is a modern approach to device description, device integration and lifecycle management for CIP technology. The xDS concept will be extensible as CIP technology and automation systems evolve into the future.

This white paper will provide the reader with an understanding of the background building blocks that are going into the development of the xDS concept. How the xDS concept will be used in future systems will be shown. It will not be an exhaustive look at all the uses for the xDS concept but will tease the reader with the basic features to be incorporated into the xDS concept. The actual development of xDS will exceed the features and uses discussed in this paper.

The paper will explore the lifecycle of the xDS concept, largely referenced by the xDS file, through the eyes of the different consumers. It will start with the generation of the files by the device vendor and move through the certification and consumption scenarios. Afterwards it will go through the traditional

automation tools such as engineering, operator and maintenance stations. In addition it will touch on the impact of some emerging technologies like TSN and the IIoT architectures.

General Discussion

Some general information concerning the xDS concept is needed before one dives into the operational aspects of the concept.

The xDS concept can be thought of as an information model for the device to which it is associated. Beyond a simple device description, this information model contains much more than just the register map and supported objects and attributes for the device. This information model will describe the how to represent the associated device to the overall system. The operations that can be supported by the device will be included in the model. The relationships to other devices that can be supported by the device will be defined. Shareable data and the organization of that data will be part of the information model. Relevant documentation can be located either within the model or by proxy through the model.

A digital twin is an idea that has become pervasive inside of industrial automation systems. (This can be a discussion all by itself.) The xDS concept is a construct that will be consumed by a system tool to feed or support the digital twin. In some cases where the device is very simple or the system is very simple the xDS concept may be the digital twin or enough of a twin to support that system.

How the xDS concept is used by the system tool must not be specific to that system tool. The xDS concept must be agnostic in relation to its consumption by the tool. There must be no specific requirements or translation burden put on the tool to use the xDS concept.

Data in the xDS concept needed by system tools must be available to the tool in real-time relative to the operating speed of the industrial application supported by the tool. Some systems operate at such rates that fetching data proxied by the xDS concept is not practical. The xDS concept must be able to bring the data and information model information to the system tool at a rate such that the system can easily support the device connections within the system, whatever may be that information.

Security of the xDS concept will be a major consideration in all facets of its lifecycle and usage. Cyber-security, physical security and security around its usage are paramount. Encryption of the parts of the concept will be considered where it makes sense. For usage, Role-Based Access Control can be employed to ensure that persons using the concept only have access to those parts needed for that person to perform her or his prescribed duty. The operator may only need to access the parts concerning system operation or may need complete access to the information. The maintenance person may only need access to other parts. Only allowing access to the part of the concept needed for a specific function will protect it from tampering and will protect the system in which the xDS concept is being consumed.

In the past ODVA has used the STC file to develop and support the conformance testing of a device. Using the xDS concept there will be no separate file support for conformance testing. The elements of the STC file will be incorporated into the xDS concept. All the feature and information needed about the device for the conformance work flow will be an integral part of the xDS concept.

Descriptors

The figures in the following discussion will have a specific convention. Tools shaded in orange will be created and provided by ODVA. Vendor developed tools and products are shaded in green. There will be multiple vendors producing products and tools used in the same architecture. The parties involved in the reference architectures are identified. The deliverables for each party are listed in the dialog.

We will focus on the following different points of view in this document:

- Common Device Vendor View Point
- Device Vendor View Point with TSN

- Conformance Test View Point
- Application Developer View Point
- TSN Capable System Development View Point
- Maintenance View Point for Console and Handheld Scenarios
- IIoT View Point

Common Device Vendor View Point

Creation of the xDS artifacts related to the overall concept will be the responsibility of the device vendor. To that end, the device vendor will create, maintain, and produce the electronic signature for the xDS artifacts in the form of a file.

The device vendor must conformance test and certify the device and the associated xDS file through the ODVA Conformance Authority. The certification of the device and xDS file by ODVA are required.

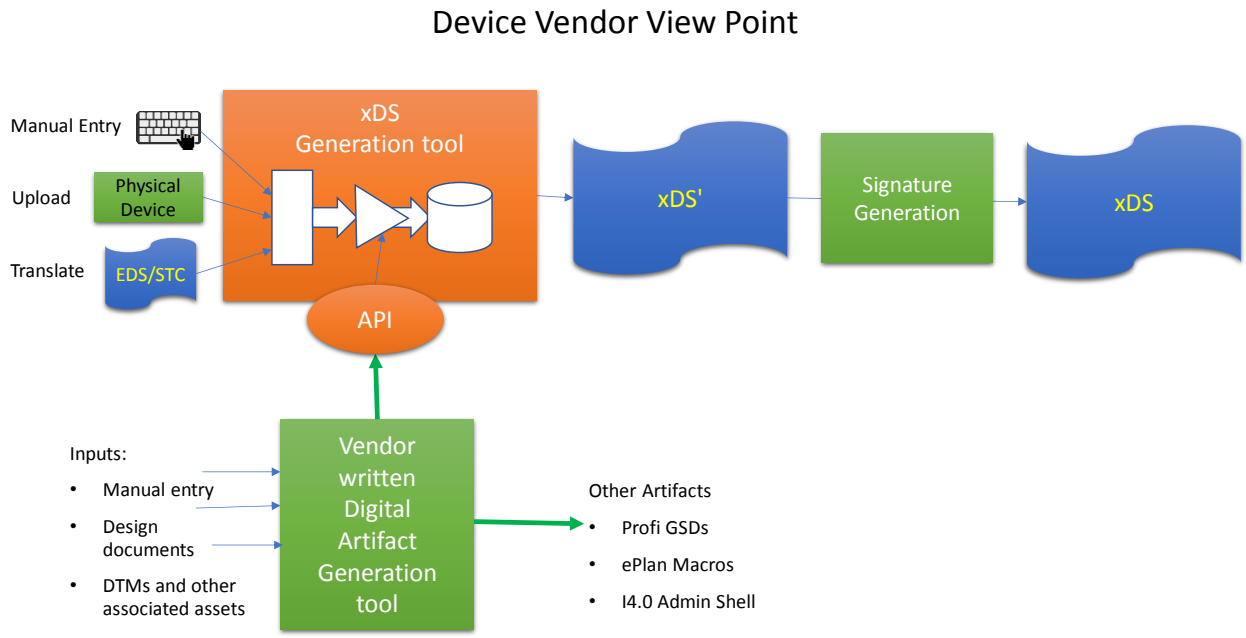

Figure 1: A view showing how the device vendor would create an xDS file.

The device vendor is fully responsible for the xDS file. The ownership of the xDS file and the signing authority of the xDS file belongs solely to the device vendor. All legal responsibility for the xDS file remains with the device vendor. Once the xDS file has been signed by the device vendor the xDS file cannot be changed without going back through the device vendor signature process. A new electronic signature would be required for the updated xDS file.

To support development of the xDS file, ODVA will provide an xDS Generation Tool. The xDS file generated by the ODVA Generation Tool is not an electronically signed document right out of the tool. We refer to this file as the xDS' (xDS prime) file. As such it is not ready for conformance testing. The device vendor must electronically sign the xDS file for the file to ready to be conformance tested.
There will be an API provided by ODVA that will be openly described for the device vendor. The device vendor will be free to invoke this API from any external tool. The API will trigger the data validation and

serialization functions in the xDS generation tool. The device vendor is free to develop and use a vendor artifact generation tool that interfaces to the ODVA xDS generation tool through the API to aid in the development of the artifact.

Generation of an xDS for existing devices can be accelerated by use of two input interfaces into the xDS generation tool. One interface discovers the internal object model of the device through use of EtherNet/IP services. The other interface will translate the EDS and/or STC files for a device.

The tool can also be entirely driven by manual entry through a graphical user interface.

All of these mechanisms will be able to be used in conjunction with one another to create a single xDS file.

The xDS Generation tool will support the ability to encode the following types of data.

- Public data used for user configuration and ownership of the device including required, optional, and vendor specific parameters.
- Encrypted Private data considered protectable intellectual property with contents and access rights controlled by the Device and/or Host Vendor. The encrypted private data must not affect the usage of the xDS file by those vendors that do use encrypted private data.
- Hidden (not exposed to the user or tools) Conformance data required for the purpose of conformance test but not intended for use by end-users.

The device vendor signed file (xDS) is still not ready for use in an automation system as it must go through the conformance testing and be certified by the ODVA Conformance Authority to be used in an automation system. This will be discussed below.

Device Vendor View Point with Products supporting Time Sensitive Networking (TSN) Capabilities

TSN is an emerging communication technology that will have a significant impact on industrial automation systems. Therefore, it is necessary to anticipate the development of the xDS artifact in relationship to TSN. The following view point explores the minimal needs that TSN technology will place on the xDS artifacts and the generation of the xDS file.

For a device vendor that supports a TSN capable device, it is expected that the TSN configuration information associated with the device will be included in the xDS file.

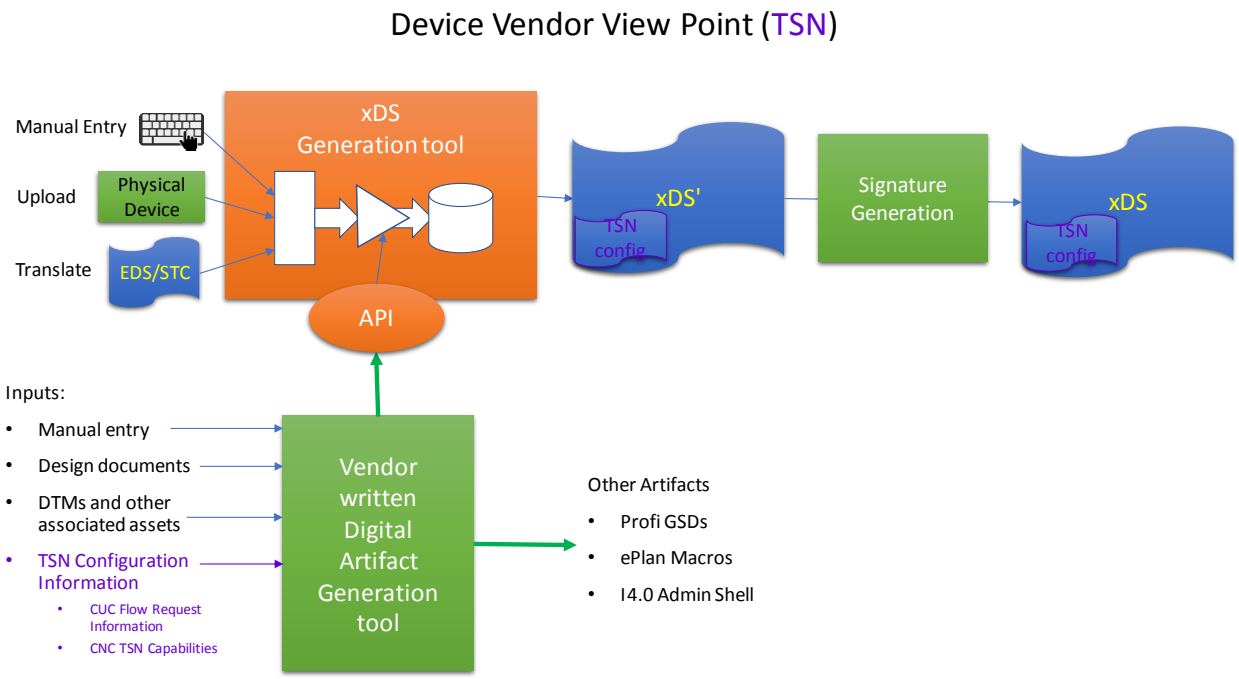

Figure 2: A reference architecture for a device vendor when the device supports TSN capabilities

The TSN Configuration Information will include the Central User Configurator (CUC) Flow Request Information and the Configurator Network Configurator (CNC) TSN Capabilities. The CUC Flow Request Information may include its talker/listener identity, communication frequency, availability requirements, latency/jitter requirements and any other information needed to establish a TSN flow. The CNC TSN capabilities included in the xDS file may include switch fabric latency, link speeds, PTP precision, possible cable connections, and any other information concerning network topology configuration.

Conformance Test View Point

xDS will impact the conformance process of ODVA. The EDS file is needed for conformance testing and is checked. However, the requirements surrounding the EDS file for conformance are light. One can even use a “generic” EDS file for a device and still pass conformance testing. That will change with the adoption of the xDS concept. The xDS concept and the files from this concept will require greater testing and much stricter accountability both for the device vendor and the ODVA Conformance Authority.

The ODVA Conformance Authority will be responsible for the validation, verification, and certification of a device vendor’s xDS file. The ODVA Conformance Authority will be responsible for maintaining the certification and Declaration of Conformity for the device vendor’s xDS file.

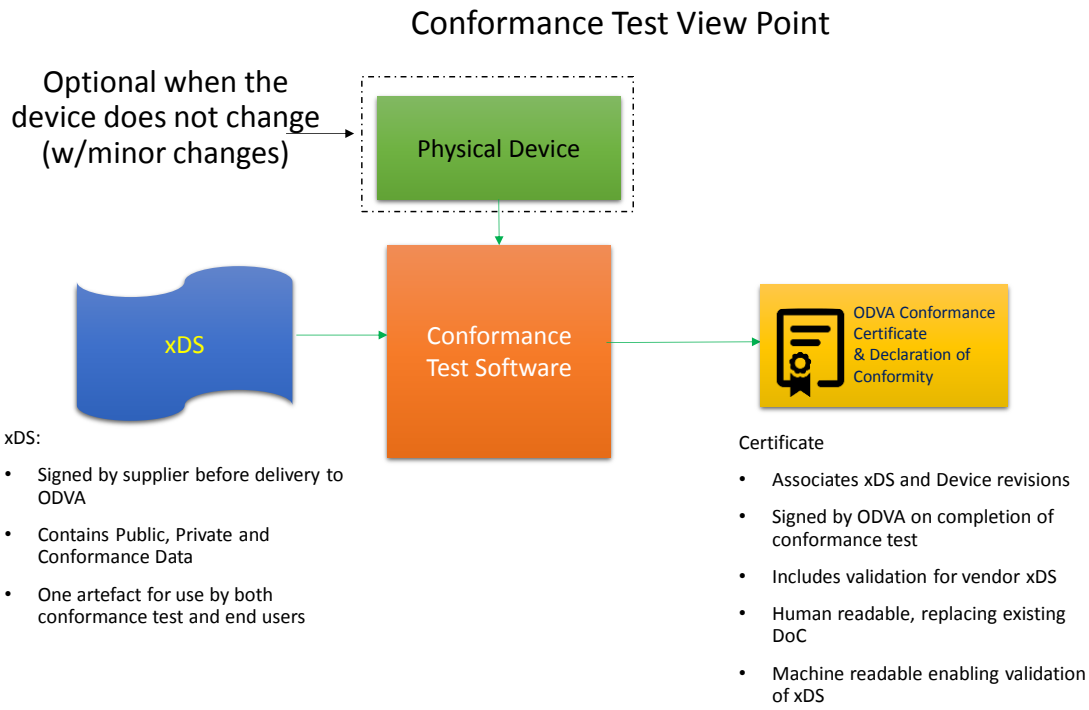

Figure 3: This diagram shows how the ODVA Conformance Authority will test, validate and process the device vendor xDS file.

The ODVA Conformance Authority will receive the xDS file as signed by the device vendor. Unsigned xDS files from the vendor will not be accepted or tested.

ODVA will conformance test the xDS file then sign the Conformance certification and documentation for the xDS file before the file is released and stored. ODVA maintains the certificates. ODVA will create a cryptographic HASH to protect the integrity of the ODVA specific content in the xDS file.

Certificate and Declaration of Conformance (DoC) will most likely be a single electronic document with human readable and machine-readable elements. It is necessary that the DoC be human readable to allow potential purchasers to confirm the device has been conformance tested, certified before purchase, and can also be included in final system documentation as part of the system statement of compliance.

The machine-readable certificates will allow automated validation insuring the xDS file deployed in a project has passed conformance test. In order to successfully validate an xDS file both the vendor's and ODVA signatures must be checked.

The xDS file from a device vendor can be conformance tested and certified independently from the associated device. This allows a device vendor to upgrade an xDS file without any associated change to the device firmware. This type xDS upgrade does not require to retest the device. The xDS file must be retested and a new certificate must be issued but the process should be streamlined such that the device is not required. Previously certified xDS files must continue to be validated and approved. (There will be devices using the original xDS file and the same version of the hardware therefore the xDS files all versions must be maintained.) The vendor can deprecate the previous xDS file but ODVA cannot. It is a vendor decision.

Application Developer View Point

The Application Developer will use the xDS file provided by the device vendor and certified by the ODVA Conformance Authority. The xDS file will be used by the System Configuration Tool under the guidance of the Application Developer.

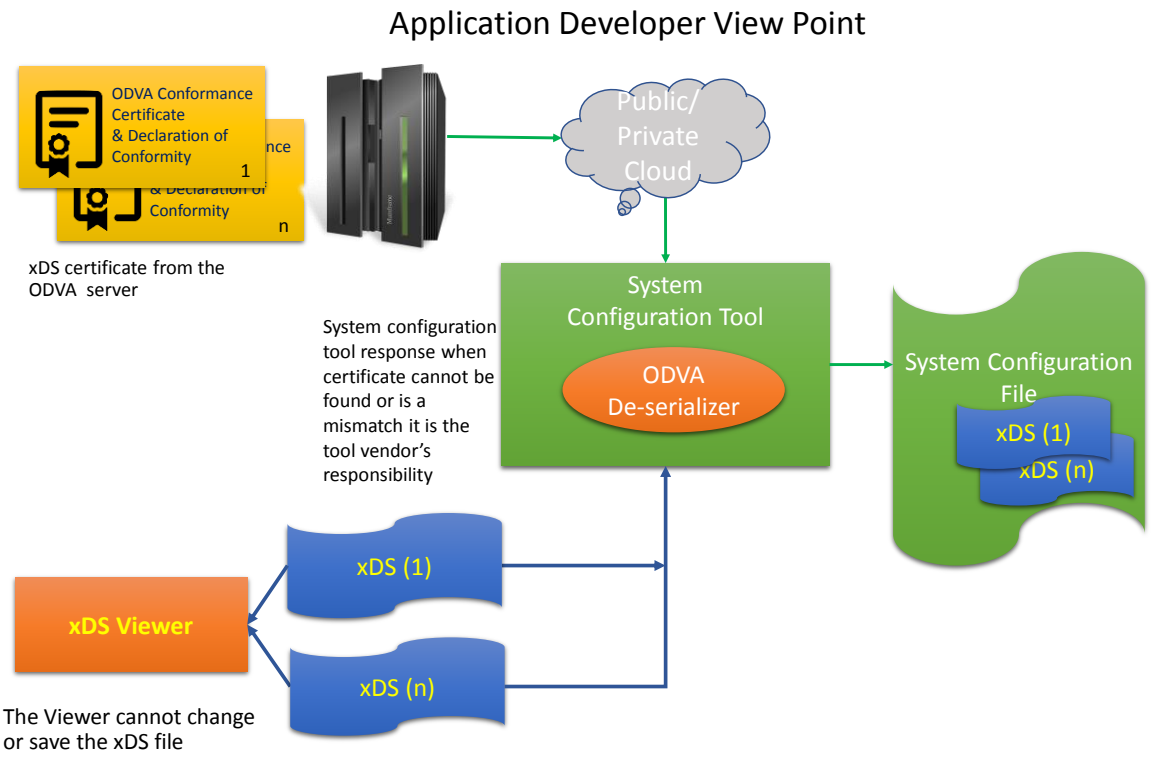

Figure 4: The operations and tools available to the Applications Developer for using the xDS file.

It will be up to the Application Developer to insure that the xDS file provided is certified by the ODVA Conformance Authority by whatever means available to the Application Developer.

Actions required when the certificate cannot be found or is not available are defined by the System Configuration Tool vendor. The Application Developer must decide how to proceed with development based on the tool vendor's actions should the xDS file be unable to be verified.

The Application Developer is not able nor allowed to change the xDS file, nor can the Application Developer alter the certification files associated with the xDS file.

ODVA will provide the software "de-serializer" function to the System Configuration Tool Vendor for incorporation into the System Configuration Tool. This de-serializer function is expected to be Operating System (OS) independent and compiler independent and therefore not require compiler options. The de-serializer will only operate on the public data within the xDS file. The de-serializer will not use or alter the encrypted private data in an xDS file should the file contain encrypted private data.

ODVA will provide an xDS Viewer tool that is OS independent, compiler independent and does not require compiler options. The viewer will only operate on the public data within an xDS file. Any attached encrypted private will not interfere with the viewing of the public data.

Viewing of encrypted private data will be subject to the company that generates this data. The company that generates encrypted private data that is attached to an xDS file will provide any tools needed to view the data by those third parties that are privileged to view the private encrypted data independent of the ODVA xDS Viewer Tool.

TSN Capable System Application Development View Point

The application developer of an automation system that is TSN capable will use xDS files with TSN information support. It is expected that the system configuration tool will be able to utilize the TSN information provided in the xDS files.

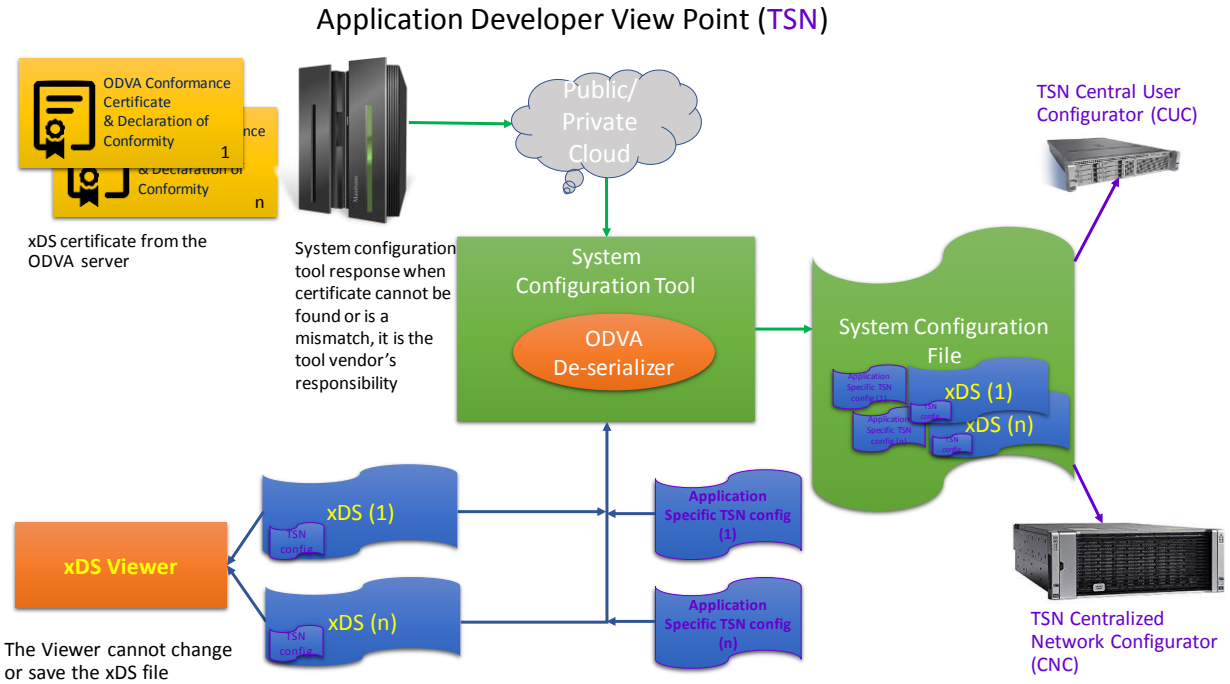

Figure 5: The operation and tools available to the application developer for a TSN capable automation system. The system configuration file should be able to interface to a TSN CNC and CUC.

The application developer will have the capability to add to and/or update the TSN configuration data of the TSN capable devices in the system. In effect, the application developer will be able to tailor the TSN configuration of devices to the specific needs of the TSN capable system. Specific TSN configuration data may include different talker/listener identity (IP address for example), a specific communication frequency, or other tailored information for the actual automation system and network configuration (such as not allowing preemption if desired).

The TSN configuration data is expected to be consumed by the CNC and CUC within the automation system.

As the use of TSN technology becomes better understood, the information useful to the TSN system may change. Those changes will be reflected in the TSN content available in the xDS file.

Maintenance View Point for Console and for Handheld Scenarios

The xDS file will need to be maintained over the lifecycle of the device to which it is associated. The xDS file must also fit into the lifecycle of the end-user's system in which it is being used. In general, there are two scenarios that cover the maintenance consumption of the xDS file, the system where the console is the main interface to the automation system and a system where some other means may be available for the maintenance of a system such as a handheld device.

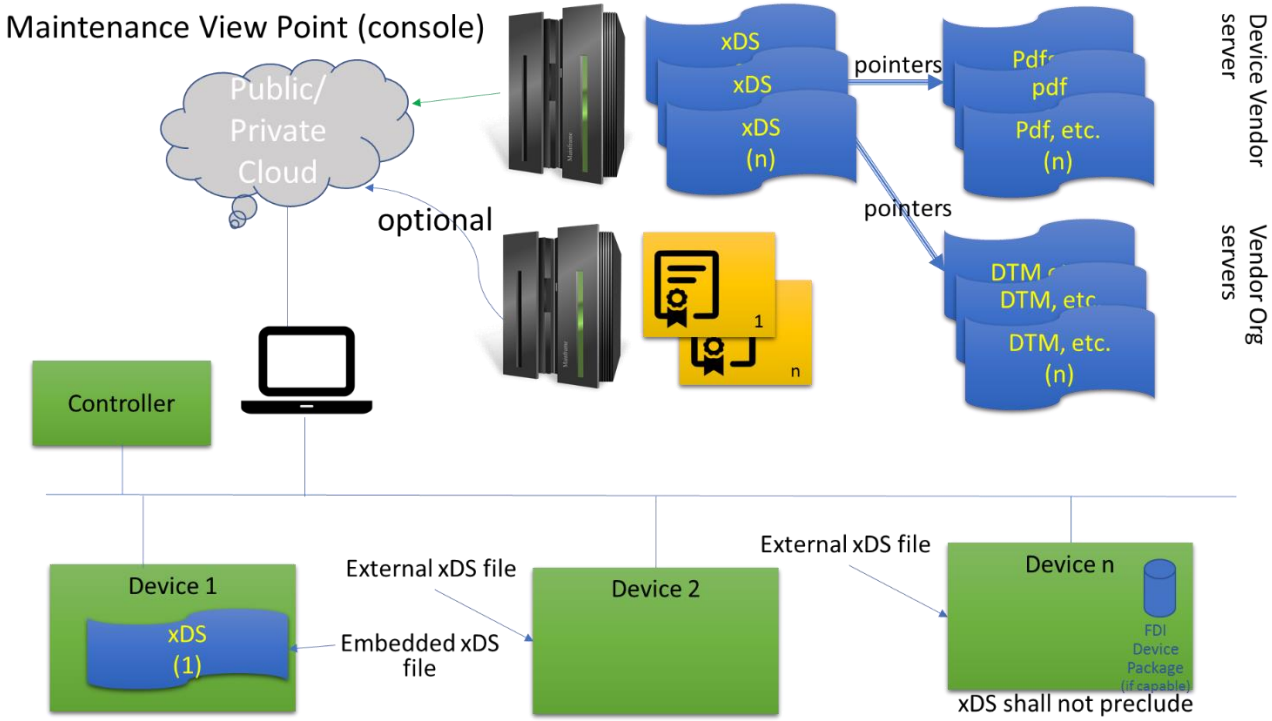

Figure 6:This diagram shows how the xDS file can be used during maintenance and operation in the end-user's system through a maintenance console.

The device vendor that owns xDS file is responsible for providing the signed and certified version of the xDS file to the end-user. (ODVA only maintains the certifications for the xDS files.) The xDS file can be embedded in the device, located on premise electronically, or using external cloud technology.

As noted in Figure 6, the xDS artifacts shall be convertible into a FDI Package by use of an xDS consumption tool.

Any reference links such as a Uniform Resource Indentifier (URI) to the xDS file and supporting documentation (DTM's, product information, etc.) must be maintained by the device vendor. The handling of broken links to an xDS file and other documentation will be the responsibility of the device vendor providing the file and information.

The repository for the device support documentation can be on multiple server locations and maintained by different responsible parties. This is not the responsibility of ODVA.

It will be left to the end-user to decide whether or not to verify that the xDS files for the products being used by the end-user have been certified by ODVA. ODVA will provide electronic access to the certification information for the xDS files.

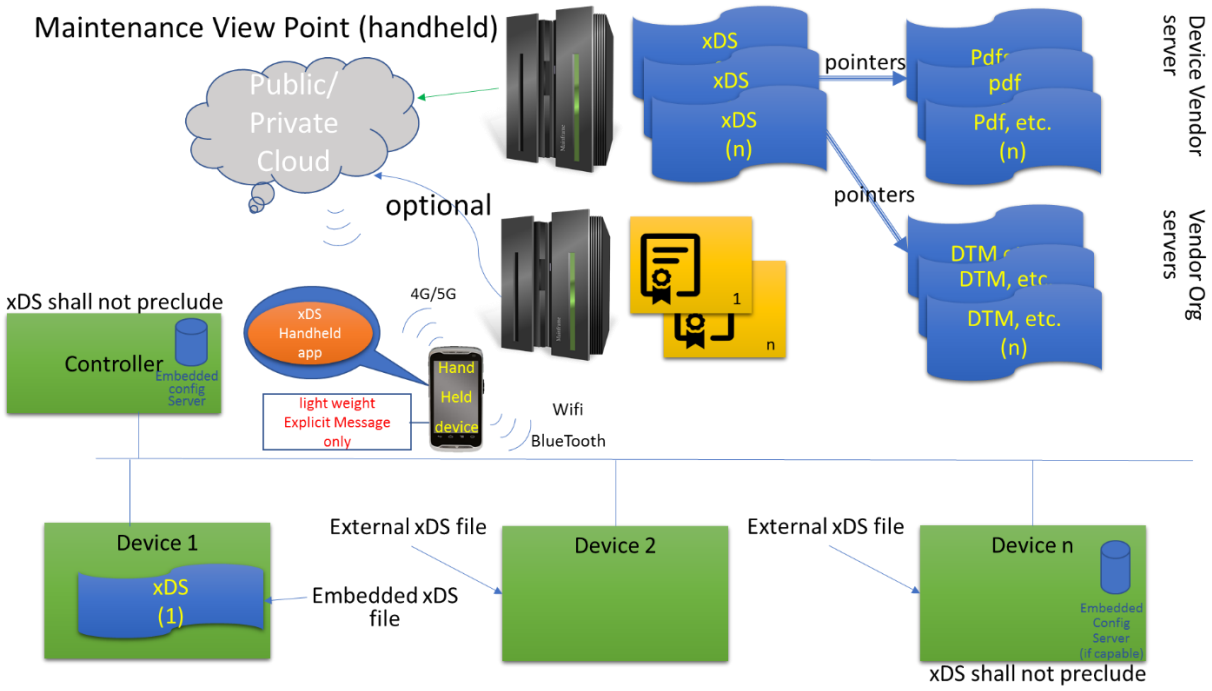

Figure 7: This diagram shows how the EDS file can be used during maintenance and operation in the end-user's system for handheld operation.

The user experience in this scenario is essentially the same as with the console maintenance architecture. The main differences are how the handheld device interfaces to the system and the more constrained resource limitations of a handheld device compared to the console.

The handheld device should support WIFI, Bluetooth and cellular technology and should support mobile friendly technology. The mobile friendly technology is likely to include HTML5, Java, JSON, and emerging IETF standards. Without this support the handheld device will have difficulty operating in a modern automation system.

Use of cellular wide area networking is also an emerging technology. This implies comparatively low bandwidth and low reliability connectivity. It also requires a complex authentication process.

This scenario assumes the separation of client and server for the user interface and therefore there is a separation of data and metadata.

This scenario will likely drive to a user interface that is not natively hosted on the handheld device. As an example, this scenario will not preclude the use a FITS (FDT IIoT Server) on a device.

IIoT View Point

Modern automation systems are built around the concept of the Industrial Internet of Things (IIoT). The xDS file will be designed to interoperate with the modern aspects expected in an IIoT system.

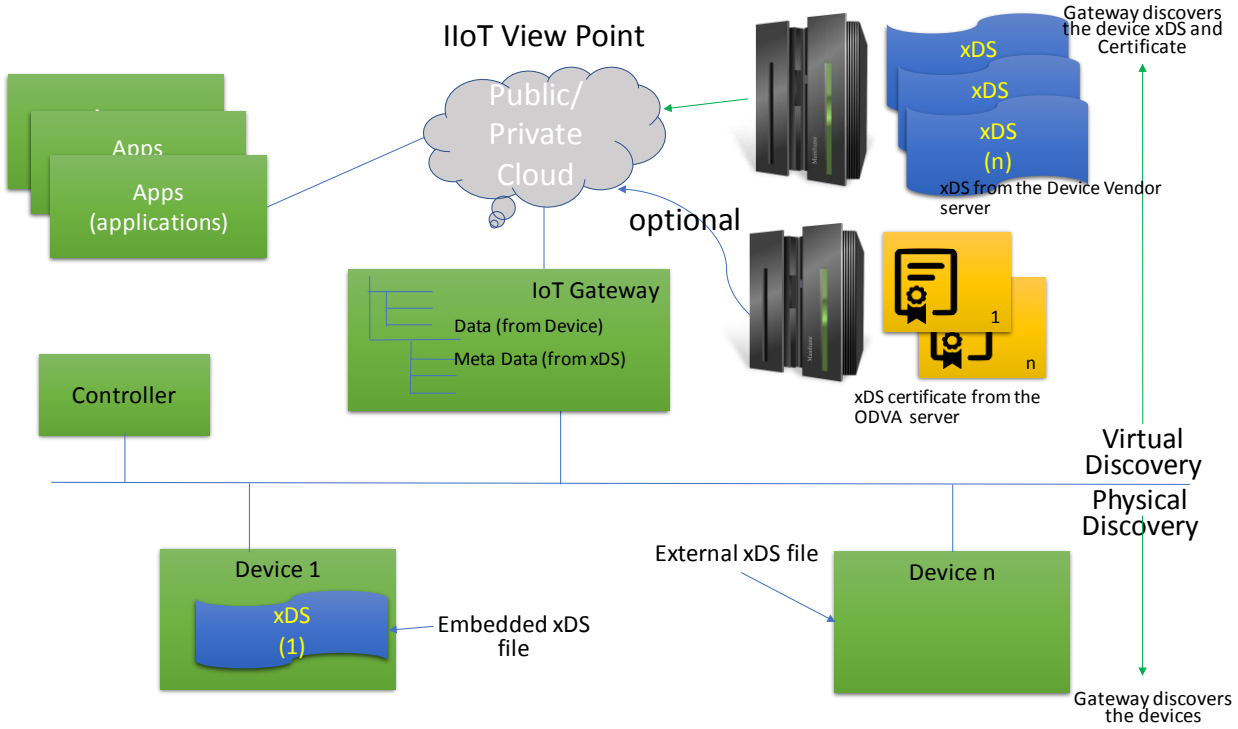

Figure 8: An overview of xDS file usage over an industrial automation system that utilizes the modern aspects of an IIoT based system.

The xDS file is owned, signed and maintained at the Device Vendor's server as stated earlier. No one in an IIoT automation system can modify the signed xDS file, including the Device Vendor. The integrity of the xDS file is an important feature of the xDS concept.

ODVA is responsible to provide the certification of an xDS file to the end-user. ODVA will provide electronic access to xDS certifications and proof of conformance testing, the DoC.

It is the responsibility of the system end-user to verify the certification of the xDS files used in the system. There is no enforcement of the certification verification process.

The end-user can use applications from any party. It is suggested that the end-user only use applications from a trusted party.

The user of IoT software has little interest in the gateway and is primarily focused on the end device. The device vendor may want to define how their device is presented to the client. Therefore, the xDS file shall be able to include related but independent artifacts such as OPC UA nodeset files.

Conclusion

The xDS concept will become an important feature in the operation of CIP networks, such as EtherNet/IP or any other applicable protocols, in the near future. The impact of xDS will cross the entire lifecycle of the associated device. The EDS file and usage will be replaced by the xDS concept and the delivered artifacts.

Flexibility in the usage and adaptation of the concept is needed to work in the CIP networks as those networks are also adapting. TSN technology, Digital Twin technology, new protocols will be introduced

and other impacts are coming to the CIP networks. The xDS concept must be able to work with these impacts without significant change to the concept.

Throughout the paper it was stated that the device vendor owns any xDS artifacts needed for their devices and holds all the responsibility for those artifacts. Further, the device vendor must electronically sign the xDS artifacts before sending them to ODVA. The xDS artifacts must be conformance tested and certified before the artifacts can be used in a CIP network, with caveats stated below. Storage and accessibility of the xDS artifacts is also the responsibility of the device vendor. A consumer of the xDS artifacts will contact the device vendor for these artifacts. It is strongly recommended that the device vendor keep old revisions of the xDS artifacts to support older versions of their products still being used in the field. Deprecation of old revisions can be done by the device vendor and the vendor will be responsible to advise their customers of this action and how to handle the deprecation process. Once the xDS artifact is electronically signed, the artifact cannot be changed throughout the lifecycle of the artifact.

ODVA is the Conformance Authority for the xDS artifacts and will only accept electronically signed artifacts. Conformance testing and certification of the xDS artifacts is the sole responsibility of ODVA. ODVA will maintain a repository of the Conformance Certificates and the Declaration of Conformance for the xDS artifacts. This repository will be accessible to the consumers of the xDS artifacts.

The burden of usage of the xDS artifacts lies with the end-user. It is recommended that end-user only accept xDS artifacts that have recorded Conformance Certificates and DoCs. However, the end-user may use any xDS artifact as desired. ODVA will not police xDS artifact usage but recommends the use of certified sources. The end-user will contact the device vendor for the xDS artifacts related to the specific device or devices being used. For the associated Conformance Certificates and the Declaration of Conformance for the xDS artifacts, the end-user will contact ODVA.

This paper described the basic scenarios that make up the lifecycle of the xDS artifacts and the xDS concept. We started with the origination of the artifacts and the certification process then led the reader through the basic lifecycle stages. Not all scenarios could be covered in the paper. The device vendor, ODVA, application developer all have roles concerning the xDS concept and the derived artifacts. Topologies for the automation systems to consume xDS artifacts were shown with some of the impact expected by new technologies. xDS is going to be a significant tool to support CIP networks (EtherNet/IP, etc.) in the very near future. Its impact will be much more than a simple device description tool or file. xDS is expected to remove some of the complexity the new networking topologies that are coming to CIP and to automation systems.