SICE Annual Conference 2011
September 13-18, 2011, Waseda University, Tokyo, Japan

OPC UA Information Model, Data Exchange, Safety and Security for IEC 61131-3

Iko MIYAZAWA[1], Masashi MURAKAMI[2], Takashi MATSUKUMA[2], Koji FUKUSHIMA[3],
Yoshiharu MARUYAMA[3], Masayoshi MATSUMOTO[3], Junichi KAWAMOTO[4] and Eiji YAMASHITA[5]

PLCopen Japan (http://www.plcopen-japan.jp/)

Abstract: Data exchange, safety and security are required in many measurement and control systems in which programmable logic controllers are used in recent days. In this paper, we will describe the IEC 61131-3 software model at the first, and then introduce the method to translate this model to the information model of OPC UA. We will also mention that the translation between the models will be based on the each XML schema easily. Next, we will explain the safety software Function Blocks (FB) defined by PLCopen and show that the safety software applications can also be easily represented by the information model and their data can be shared by the monitoring systems. Finally, we will discus the security of PLC programming using OPC UA.

Keywords: OPC UA, Information Model, Data Exchange, Safety, Security and IEC 61131-3.

1. INTRODUCTION

In recent years, various networks have been used anywhere in any time. This is a situation similar to industrial world where many kinds of industrial networks have been used such as in the fields of Process Automation (PA) and Factory Automation (FA). A major feature in these fields is that many kinds of networks may be used simultaneously in a same plant and different types of them used in different layers of various systems. To exchange data smoothly within these networks is a problem in a typical industrial plant. And visualization of such plant is also required in recent days. A powerful approach to solve this problem is using OPC methods provided by OPC Foundation. Especially, the newest promising method is OPC UA (Unified Architecture) which is intended to exchange data in object data models [1].

On the other hand, the programming languages of PLC (Programmable Logic Controllers) are defined in IEC 61131-3 and this standard has been widely used in industrial field [2]. PLCopen is a vendor and product independent worldwide association to support the use of this standard in this field. PLCopen has released a technical specification, "XML Formats for IEC 61131-3" 6 years ago, which is a kind of XML schema to describe the PLC programs in the XML formats. With this technical specification, it is expected that the PLC programs can be exchanged smoothly among different PLCs and the portability of software applications of PLC will be achieved. The practical situations needed data exchange are not only performed within PLCs, but also with controllers and various field devices.

[1] Kanagawa Industrial Technology Center
Tel : +81-46-236-1500
E-mail: miyazawa@kanagawa-iri.go.jp
[2] Digital Electronics Corporation
[3] Fuji Electric Corporation
[4] Toshiba Corporation
[5] Yokogawa Electric Corporation

And a main purpose of data exchange is required and also often used in monitoring systems. Data exchange is indispensable to monitor a system to know its situation in any time.

In this paper, we will describe the IEC 61131-3 software model at the first, and then introduce the method to translate this model to the information model of OPC UA. We will also mention that the translation between the models will be based on the each XML schema easily. Next, we will explain the safety software Function Blocks (FB) defined by PLCopen and show that the safety software applications can also be easily represented by the information model and their data can be shared by the monitoring systems. Finally, we will discus the security of PLC programming using OPC UA.

2. INFORMATION MODEL

Fig. 1 shows the IEC 61131-3 software model and this model and its contents can be represented in an XML format defined in the technical specification of PLCopen.

A measurement and control system consists of devices in the definition of IEC 61131-3. A device has more than one resource and resource can be a PLC in most systems. A resource is a controller and software application must be running inside of the resource. The execution of software application has been defined as a task and a task can be programs or Function Blocks (FB) or their combinations.

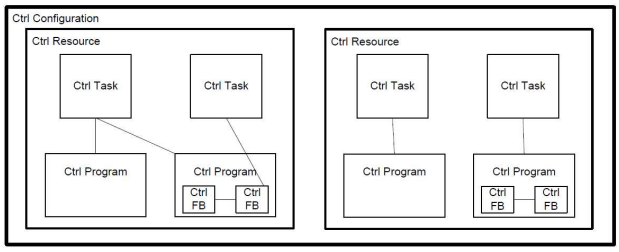

Fig. 1 Software model of IEC 61131-3

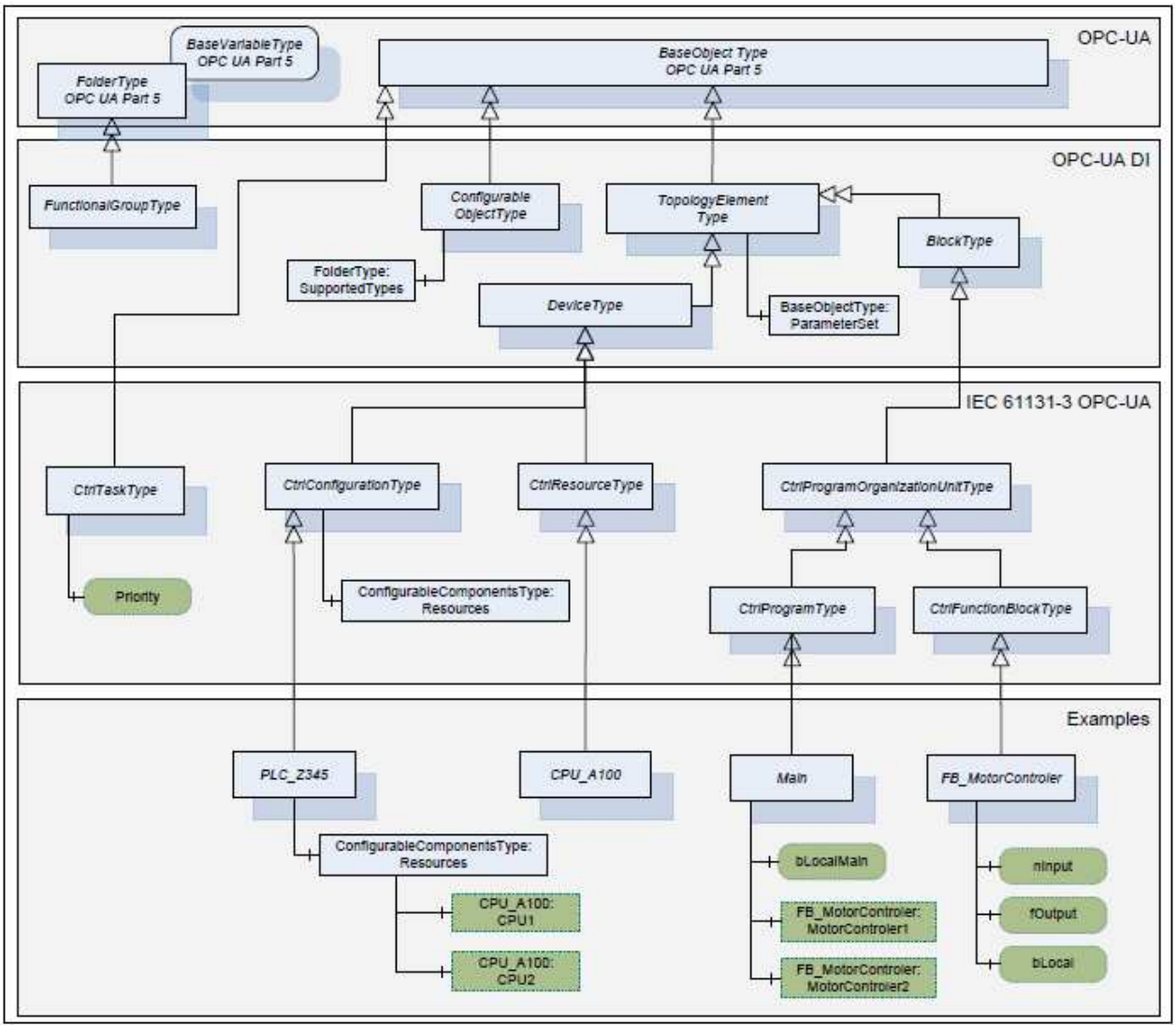

Fig. 2 OPC UA information model

Fig. 1 is the configuration of software of a measurement and control system. In Fig. 1, the prefix Ctrl is used to show the elements or contents in IEC 61131-3 [3]. Ctrl is a representation of OPC UA for IEC 61131-3 and the elements next to Ctrl are simply described by IEC 61131-3. Here, the software model has been depicted as a configuration in which the executing tasks and several Program Organization Units (POUs) have been shown.

Fig. 2 shows the OPC UA information model defined by OPC Foundation [3]. There are four layers defined in this figure, and the two layers on top are the OPC UA related layers. In the 3rd layer, the link between IEC 61131-3 and OPC-UA is depicted. Here the elements of the IEC software model are shown, in which the elements of software model are mapped on the lowest layer to the control architectures.

It is shown in Fig. 2 that the prefixes of Ctrl can be understood as interfaces between OPC UA and IEC 61131-3. In the 3rd layer, objects shown with Ctrl, CtrlTaskType, CtrlConfigurationType, CtrlResource-Type and CtrlProgramOrganizationUnitType are mapped to the elements of OPC UA in the 1st and 2nd layers.

Fig. 3 shows an example of POU type. In this example, a POU as CtrlProgramOrganizationUnitType is mapped to BlockType, i.e. a sub object of BlockType. Under the CtrlProgramOrganizationUnitType, there are the elements of IEC 61131-3. In the left side, its task, body and SFC have relevance to the declaration of bodies of POU. In the right side, the variables are shown.

In a real case, the data of a PLC are represented with variables of POUs. The data structures of a PLC are declared in each declaration part of POUs. A declaration has two main parts, the head of POU including the variables, and the body of POU including the codes of programs. And all the declarations are performed its configuration of the PLC.

When using the OPC mechanism to exchange data within devices, it does not need to define any other data structures over any networks. It is just required to construct an OPC UA server and the data exchange is executed through that server.

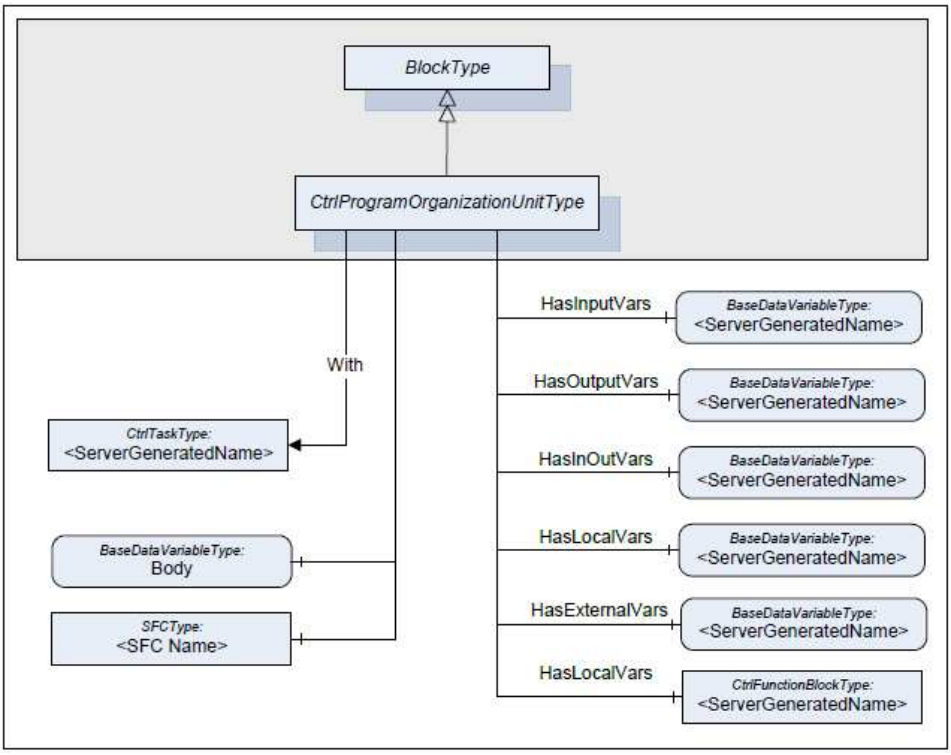

Fig. 3 The overview of POU type

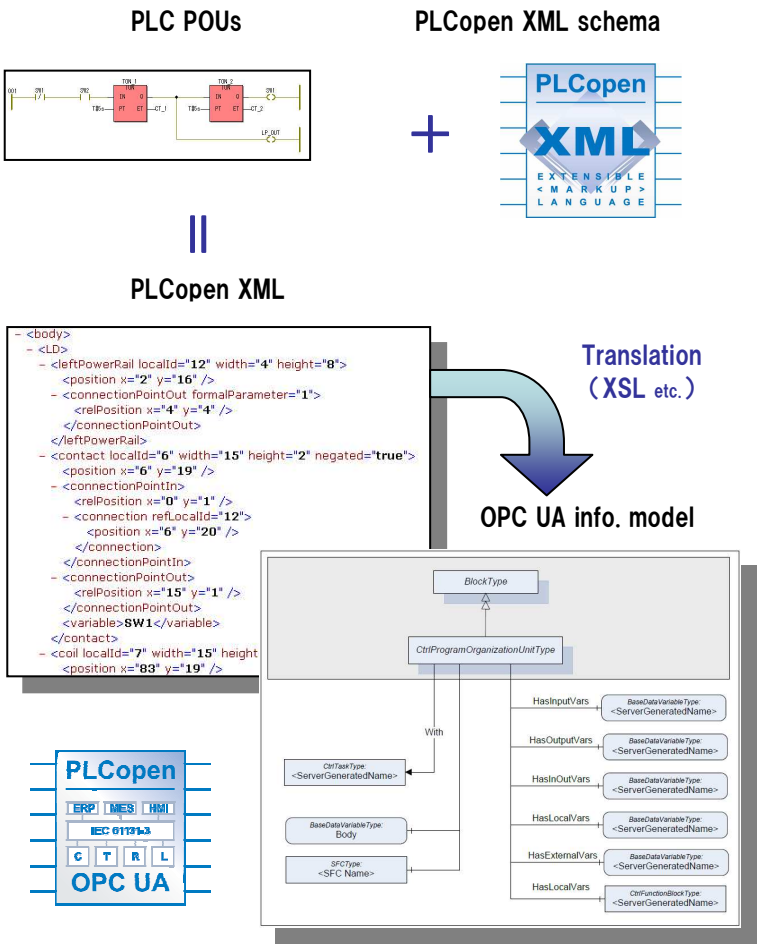

Fig. 4 The practical use of XML schema

3. DATA EXCHANGE

In the above section, we have seen that the data of a PLC have been represented in POUs defined in IEC 61131-3, and these data have been mapped to the information model of OPC UA. In this section we will express the method to translate the data from IEC 61131-3 to OPC UA.

The real data of PLCs produced by different venders must have the different formats. It is not so easily to translate the data between the different PLCs. The PLCopen, however, has defined the formats of eXtensible Markup Language (XML) for IEC 61131-3 [4]. If a PLC uses this XML formats to represent its data, the data exchange can be executed through the XML Schema Document (XSD) defined in [4].

On the other hand, OPC UA also has XML formats [1]. It is well known that the data exchange between XML formats can be conducted by eXtensible Stylesheet Language (XSL) to just exchange the XML formats.

Fig. 4 shows the practical use of XML schema to translate the XML representation of IEC 61131-3 POU to OPC UA information model.

4. SAFETY

Safety when using PLCs has many aspects including hardware and software. IEC 61131-6 will define hardware aspects for the use of PLC safety, so this aspect will be beyond this paper. We just discuss the software aspects here.

PLCopen has defined safety related aspects within the IEC 61131-3 development environments [5]. With this technology, the safety aspects can be transferred to a software tool, which is integrated into the software development tools.

In [5], a new BOOL data type, SAFEBOOL has been introduced as a strongly recommended new safety-related data type for binary safety signals only. Adding this new data type into the information model, we can represent the data related to safety aspects and exchange them among the systems.

The contents of the functionality of safety must have been implemented in relevant FBs. So the data related to safety must also have been represented in such FBs, and as saw in the above section, the safety related data should be transfer to other systems in the information models adding a new data type called SAFEBOOL. These modifications are just done under the layer of OPC UA information models, so there is no any difficulty to translate the safety data to other devices or monitoring systems.

The main technology of PLCopen Safety functionality is to define 20 kinds of safety functional FBs [5]. These FBs will be represented in the form of XML and can be translated to OPC UA information model. For example, the FB called Emergency Stop has the input and output variables as shown in Table 1.

Table 1 The variables of Emergency Stop FB.

Name	*Data Type*	*Initial Value*
VAR_INPUT		
Activate	BOOL	FALSE
S_EStopIn	SAFEBOOL	FALSE
S_StartReset	SAFEBOOL	FALSE
S_AutoReset	SAFEBOOL	FALSE
Reset	BOOL	FALSE
VAR_OUTPUT		
Ready	BOOL	FALSE
S_EStopOut	SAFEBOOL	FALSE
Error	BOOL	FALSE
DiagCode	WORD	16#0000

The variables in Table 1 will be mapped to the information model shown as Fig.3 and data will be accessed shown as Fig.4.

5. SECURITY

IEC 61131-3 is a standard of programming languages for PLC. There is no anything to mention security in this standard. However, the threats of security when using information and communications technology also exist in the field of PLC. It is already pointed out that the security is a problem and there is no common method using in PLC.

On the other hand, there is a security model in OPC UA standards. Using this security model of OPC UA, it will be easily to implement security functionality in the data exchange with PLC. The OPC UA provides a standard way for servers to expose objects to clients and it will be done with a secure channel. It means that PLC just should implement the security functionality in its own part and the security of outside of PLC will be provided by OPC UA security model.

6. CONCLUSIONS & ACKNOWLEDGMENT

In this paper, we introduced OPC UA information model, data exchange, safety and security for IEC 61131-3. The authors thank the technical commission of OPC Japan for creating this article.

REFERENCES

[1] OPC UA Web Site, "http://www.opcfoundation.org/".

[2] IEC 61131-3, "Programmable Controllers — Programming languages", International Electrotechnical Commission, 2003.

[3] PLCopen and OPC Foundation, "OPC UA Information Model for IEC 61131-3", release 1.00, 2010.

[4] PLCopen, "XML Formats for IEC 61131-3", release 2.01, 2009.

[5] PLCopen, "Safety Software, Technical Specification, Part 1: Concepts and Function Blocks", release 1.0, 2006.