ISBN: 978-3-95450-237-0 ISSN: 2673-5512 doi:10.18429/JACoW-PCaPAC2022-THPP7

OPC UA BASED USER DATA INTERFACE AT ELBE

K. Zenker*, M. Justus, R. Steinbrück
Institute of Radiation Physics, Helmholtz-Zentrum Dresden-Rossendorf, Dresden, Germany

Abstract

This paper presents an OPC UA based data interface implemented at the high-power radiation source ELBE. It provides access to ELBE machine data via dedicated gateway devices.

In addition to the intrinsic security and authentication features included in OPC UA an access control mechanism was implemented at the PLC level. This allows to enable/disable user data access using the SCADA system of ELBE.

INTRODUCTION

The center for high-power radiation sources ELBE delivers different kinds of radiations serving a variety of user groups. The facility is in operation for more than 20 years and over time different machine interfaces were created for different user groups tailored to their needs. On the one hand some user groups provide experiment data like counting rates to the operators. This information is used for machine optimization. On the other hand some user groups have the permission to change certain machine parameters, like undulator gap size or beam repetition rate on their own.

So far different solutions have been used to provide those machine interfaces. Solutions include direct access to the SCADA system via dedicated accounts and OPC interfaces available in the SCADA system.

Here we present an approach of providing a common machine and ELBE data interface based on the OPC UA standard [1]. It is applicable to all use cases at ELBE and can be accessed via a single access point OPC UA server.

In the following, the infrastructure at ELBE is introduced. After the ELBE data interface (EDI) and its architecture is discussed.

ELBE INFRASTRUCTURE

ELBE is operated using the SCADA system WinCC by Siemens. The majority of ELBE systems is connected to WinCC via industrial Ethernet and proprietary S7 communication. At control level SIMATIC S7 300 and S7 400 Programmable Logic Controllers (PLC) are used. Different subsystems, like the machine protection system or the personnel safety system, and different subsets of each subsystem, belonging to e.g. different beam line sections, are implemented on dedicated individual PLCs.

The integration of subsystems based on MicroTCA.4 [2] hardware, which do not provide S7 communication interfaces, into the existing infrastructure is based on OPC UA using the open source C++ software toolkit ChimeraTK [3, 4]. Here, OPC UA allows a direct integration into WinCC using the native OPC UA support of WinCC.

* k.zenker@hzdr.de

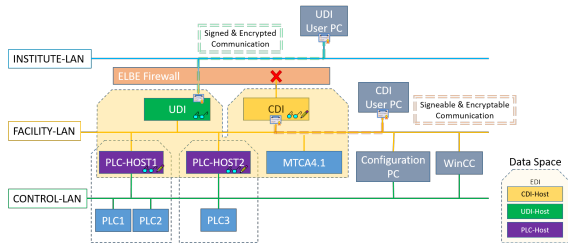

Figure 1: Overview of the ELBE data interface (EDI). The only available access points are the gateways named UDI and CDI. All other components are hidden to EDI users.

Commercially available OPC UA gateways [5] (UA Link) by IBHsoftec are used at ELBE as a data bridge between the Siemens S7-300/400 PLCs and OPC UA based applications as described in [6–8]. These UA Links are the basis of EDI.

ELBE DATA INTERFACE ARCHITECTURE

As introduced above two data sources – direct OPC UA sources like MicroTCA based subsystems and indirect OPC UA sources that aggregate PLC data via UA Links – need to be considered for EDI. Both can be interfaced by UA Links, which allows to implement EDI based on the UA Links.

From a traffic point of view it is desirable to place the UA Links as near as possible next to the PLCs in respect to the control network. Where possible the gateways have been directly connected to the according PLC interfaces. This automatically led to the introduction of several so called PLC-Host gateways throughout the ELBE machine and a multi-layer structure as introduced in the following.

Abstraction Layers

Figure 1 shows an overview of the EDI architecture currently implemented at ELBE. In a first abstraction layer of EDI are the PLC-Hosts, that are shown in the bottom part of Fig. 1. Depending on the location and the address space of the PLCs data of multiple PLCs can be aggregated by a single UA Link (see Fig. 1 PLC1 and PLC2) or a single UA Link per PLC-Host is used (PLC3 in Fig. 1). At this level the OPC UA address space is automatically generated based on the symbols defined in the PLC STEP7 project.

In general, the configuration of a UA Link allows to define the access level for each process variable on the OPC UA side. Additionally user accounts can be configured to have read only or read write access. However the available process variables are the same for each user and single process variable access cannot be defined user dependent. Furthermore, it is not possible to change process variable access during runtime.

Since UA Links at this level are not visible to the outside world it is possible to waive encryption and authentication

ISBN: 978-3-95450-237-0 ISSN: 2673-5512 doi:10.18429/JACoW-PCaPAC2022-THPP7

UDI	CDI	data structure	type	description
X	X	CURRENT.actual_value	Float	actual read back current
X	X	CURRENT.max_value	Float	maximum possible current value
X	X	CURRENT.min_value	Float	minimal possible current value
X		CURRENT.setpoint	Float	current setpoint
	X	CURRENT.SETPOINT_RW.accessible	Boolean	TRUE == write access granted
	X	CURRENT.SETPOINT_RW.value	Float	current setpoint
X	X	CURRENT.unit	String	engineering unit
X	X	STATUS.on	Boolean	TRUE == magnet current controller switched on
X	X	STATUS.ready	Boolean	TRUE == magnet current controller setpoint reached

Figure 2: Example address space of a magnet. The left two columns indicate which variables are available via the control and user data interface respectively.

for the sake of performance and ease of maintenance. They are configured to allow read and write access to PLC data.

In a second EDI layer, data from the first layer is aggregated and remapped. Here only two UA Links are present – one acting as user data interface (UDI) and the other acting as control data interface (CDI). The general difference between UDI and CDI is that UDI provides only read access to the UA Links in the lower layer, whereas CDI provides read and write access. In detail this results in a user friendly well structured address space removing any footprints from the PLC project symbols. An example can be seen in Fig. 2, which shows the data structure of a single magnet. Here it becomes clear that the address space for read only process variables is shared between UDI and CDI, whereas dedicated process variables for the current setpoint exist for UDI and CDI. This results from the PLC implementation introduced below.

The address space of UDI and CDI is created in a structured manner using UA Link local variables exclusively. They are bound to according OPC UA variables published by the PLC-Host level.

User Data Input

Additional local variables are defined at the UDI level, which are not bound to PLC-Host level variables. They are writable by ELBE users to provide information of interest for the ELBE machine operation. E.g. counting rates measured by the users are published like that and used to optimize the machine state with respect to a maximum counting rate.

User Authentication

The access point of UDI only provides endpoints that use encryption and user authentication. At ELBE a Public-Key-Infrastructure (PKI) including a ROOT Certification Authority (CA) and dedicated user group CAs has been set up that hand out user certificates based on the X.509 standard. This reduces the management effort related to the UA Links, where only the CA certificates and corresponding revocation lists need to be installed.

As can be seen in Fig. 1 CDI is currently only available for ELBE internal use inside the closed machine network. Here an endpoint without encryption and user authentication is provided. This is beneficial for debugging purposes. Once users will use CDI the endpoint will be removed and the user authentication will be similar to the one used with UDI.

PLC LEVEL IMPLEMENTATION

The PLC implementation had to respect the fact, that the ELBE machine code has been permanently extended by different developers over the last 20 years. This results in a heterogeneous data structure in respect to symbols types and scaling. To transform this source of data into a homogeneous representation it has been necessary to map the data into a well structured format already on PLC level. Even when this requires additional resources it is reasonable for the following reasons:

- Scaling information is best available and documented within the PLC project
- Data collection by the UA Links is completely transparent to the PLC developer
- The concentration to a known EDI data interface allows for easy debugging and disabling in case of machine problems
- A known symbolic data structure at PLC level allows to automate major parts of the UA Link configuration
- Misconfigurations only affect data introduced by the EDI development and not parts of the well tested present PLC code

In detail, three components are implemented for EDI at PLC level, that are introduced in the following.

Data Type and Unit Conversion

The first component converts register types and PLC internal units to physical units. The type conversion is needed because e.g. different magnet interfaces provide readbacks as different data types given in different units. Using the conversion component a consistent machine data representation can be created and exposed to users.

Write Access Logic

The second component implements write access of EDI. This access type adds significantly more complexity to EDI compared to read-only access. First of all in contrast to the read-only access, where the PLC register is simply duplicated, here two additional registers (B and C) per register to the published (A) are added. This is shown in Fig. 3. One (register B) is used to transfer data from the PLC to EDI and the other one (register C) is used to transfer data from EDI to the PLC. The PLC permanently checks for data changes of the register C and register A. Depending on whether a change in A or C is registered two different data paths are possible.

The first path is activated once a data change of register A is detected. In that case the data of register A is copied to register B, which is mapped to a corresponding process variable B' in one of the PLC-Hosts. The latter connection is a bidirectional one, which is fixed by the UA Link implementation. In the following the data is transferred to CDI via an unidirectional connection. This is possible by defining a local variable on the UA Links used for CDI. For local

ISBN: 978-3-95450-237-0 ISSN: 2673-5512 doi:10.18429/JACoW-PCaPAC2022-THPP7

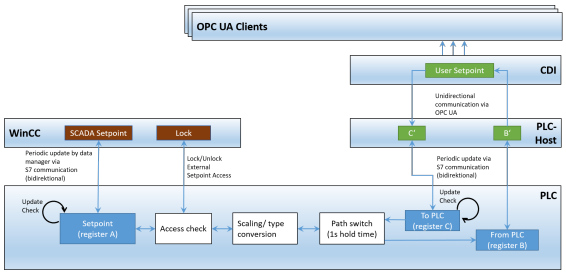

Figure 3: Write logic schematic used at ELBE. Details are given in the text.

variables it is possible to define data sources - in this case the data source is the process variable A'. At this point the data change on the PLC is visible to the user of CDI. At the same time data sinks that are to be filled on data changes of the local variables can be defined. This is used to define an unidirectional connection to the process variable C' of the PLC-Host that is connected bidirectionally with register C. The connection of C to A is interrupted as long as updates are transferred to B. It can only be closed 1 s after the last update of register A. This time is in principle defined by the time needed to transfer data from register A to register C, which includes network latency.

The second path is activated when the local variable accessible to the users is changed and the first path is not active. Now the data is transferred via register C' to C and finally copied to register A. Once this path is active no data is transferred from register A to B. This connection is interrupted as long as updates are received via register C and can only be closed 1 s after the last update of register C.

Using the approach of having two data paths and a lock time of 1 s for each direction was found to be a valid configuration at ELBE used to avoid data reflections. In case of the first path a reflection would result in overriding register A with preceding values that are transferred from register B to C. During this transfer the registers A and B could have been already updated. Similarly, in case of the second path data transferred from the CDI UA Link via register C', C, A, B and B' to CDI could override the data entered by the user in the meantime with old data.

However, our approach does not prevent data clashes resulting from different users using CDI at the same time or that result from simultaneous data changes introduced by the SCADA system, which always writes directly to register A.

Access Control

The third component is used to make sure that the SCADA system always has full control of ELBE. It adds information and controls to the SCADA system that allow to enable/disable EDI at all or just parts of it. In order to do so different groups are defined. Those groups represent different beam line section of the ELBE machine and correspond directly to subsets of the address space created in the UDI and CDI. In the end the component copies data from the registers created by the write access logic component only if the corresponding access bit is set via the SCADA system. The current access status is published to CDI via a corresponding process variable, e.g. `CURRENT.SETPOINT_RW.accessible` in Fig. 2. In addition, indicators visualizing active data changes by CDI are added to the SCADA system. This allows to distinguish between data changes by CDI and SCADA clients used outside of the control room.

PLC Timing

The components introduced above are added to a user code block of the PLC that has a fixed maximum cycle time of 150 ms. We observed an increase of cycle time by 20 ms caused by introducing EDI. This time is dominated by the write access logic related to CDI. However, the total current cycle time is 40 ms, which shows that the cycle time is still well below the limit. The Timing of time critical code executed by interrupts and high priority tasks is not affected by CDI.

CONCLUSION

At the center for high-power radiation sources ELBE an OPC UA based data interface has been established. It allows direct external access to ELBE data, which was not possible before. E.g. now users can integrate ELBE data into the experiment data acquisition or record ELBE data directly along with their experimental data. Another application of EDI is the implementation of slow feedbacks. This was successfully demonstrated in case of a beam position stabilization used to fixed the beam at sub-millimeter level on a target for a period of a week in a high power beam experiment [9, 10].

The interface is based on commercially available gateway devices that are used in a multi-layer approach. This allows to create a single access point with a configurable address space independent of the address space used at PLC level or by interfaced OPC UA servers of integrated subsystems.

On the one hand the connections to the data interface are secured by using user authentication and encrypted connections. Encryption is based on user certificates and dedicated OPC UA endpoints. A PKI for handling of user certificates was created. On the other hand the data interface is fully integrated to the ELBE SCADA system such that ELBE operators always have the full control of ELBE. This is ensured by indicators of data accesses via the data interface and the option to block selectively parts of the write accesses by data interface or to disable the write access of the data interface at all.

The PLC level implementation increased the corresponding code block cycle time by 20 ms, which left the total cycle time well below the maximum defined cycle time.

REFERENCES

[1] *OPC Unified Architecture*, The OPC Foundation. `http://opcfoundation.org/opc-ua/`

[2] PICMG, *PICMG specification MTCA.4 Rev. 1.0*, Aug. 2011. `https://www.picmg.org/openstandards/microtca`

ISBN: 978-3-95450-237-0 ISSN: 2673-5512 doi:10.18429/JACoW-PCaPAC2022-THPP7

[3] M. Killenberg *et al.*, "Abstracted Hardware and Middleware Access in Control Applications", in *Proc. ICALEPCS'17*, Barcelona, Spain, Jan. 2018, pp. 840–845. doi:10.18429/JACoW-ICALEPCS2017-TUPHA178

[4] G. Varghese *et al.*, "ChimeraTK - A Software Tool Kit for Control Applications", in *Proc. IPAC'17*, Copenhagen, Denmark, May 2017, pp. 1798–1801. doi:10.18429/JACoW-IPAC2017-TUPIK049

[5] *IBH Link UA*, IBHsoftec. https://www.ibhsoftec.com

[6] R. Steinbrück *et al.*, "Control System Integration of a MicroTCA.4 Based Digital LLRF Using the ChimeraTK OPC UA Adapter", in *Proc. ICALEPCS'17*, Barcelona, Spain, Jan. 2018, pp. 1811–1814. doi:10.18429/JACoW-ICALEPCS2017-TUPHA178

[7] K. Zenker *et al.*, "MicroTCA.4-Based Low-Level RF for Continuous Wave Mode Operation at the ELBE Accelerator", *IEEE Trans. Nucl. Sci.*, vol. 68, no. 9, pp. 2326–2333, 2021. doi:10.1109/TNS.2021.3096757

[8] K. Zenker, M. Kuntzsch, and R. Steinbrück, "Integration of OPC UA at ELBE", in *Proc. ICALEPCS'21*, Shanghai, China, Mar. 2022, paper TUPV010, pp. 400–404. doi:10.18429/JACoW-ICALEPCS2021-TUPV010

[9] HZDR press release, *Producing medical isotopes at extreme energy density*, Feb. 2022. https://www.hzdr.de/db/Cms?pOid=65365&pNid=3438

[10] DEMCON press release, *Medical radioisotopes produced with the world's most power-dense reactor*, Feb. 2022. https://dam.demcon.com/medical-radioisotopes-produced-with-the-worlds-most-power-dense-reactor