ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA158

FIRST STEP TO MANAGE MIGRATION TO SIEMENS S7-15XX PLCS USING TANGO FRAMEWORK

P. Rommeluère*, Y.M. Abiven, A. Buteau, P. Monteiro,
Synchrotron SOLEIL, Gif sur Yvette, France
S. Minolli†, Nexeya, Massy, France
P. Betinelli, CEATech, Gif-sur-Yvette, France

Abstract

Over the past years, SOLEIL [1] uses SIEMENS PLC as a standard for signal monitoring and security. SOLEIL is today thinking about a major upgrade of the facilities, and has to adapt its organization to face efficient operation and R&D. In this context, automation experts are now merged in a single group. In a middle term, migration from the existing 3XX series PLCs to the new 15XX series will be necessary. As the new 15XX series PLCs do not support Fetch/Write protocol anymore, a first step is the upgrade of TANGO [2] PLCServer. This software device ensures data exchange with supervisory applications using TANGO infrastructure. It opens multiple TCP/IP connections to the PLC hardware, manages asynchronous communication to read/write PLC Data blocks (DB) and acts as a server for other clients. The upgrade of PLCServer is based on Snap7 [3] open source Ethernet communication suite for interfacing with Siemens PLCs using the *S7* native protocol. This paper details the evolutions, performances and limitations of this new version of the PLCServer.

INTRODUCTION

When it was created in 2003, the SOLEIL synchrotron chose the TANGO software bus as the only intermediate layer between the devices intended to be read or remotely controlled and the supervision applications. In TANGO, the concept of Device Server (DS) is paramount.

Within the support groups, the use of a DS PLCServer has been standardized, as well as the SIEMENS PLC models. However, the program architectures and the structure of the DBs evolved differently according to the people in charge of programming PLCs in each groups. In 2017, following SOLEIL reorganization, automation experts were grouped in the accelerator and engineering division to offer homogeneous practices and tools to all support groups for their automation-based control systems. Approximately 250 configurations are concerned for Machine Protection System, vacuum control, Personal Safety Systems, Radio frequency, beam diagnostics and magnet power supplies.

In order to push the performance limits of the current PLCServer, but also to make it compatible with the new generations of SIEMENS PLC, it was decided to publish a new version of this DS.

* patrick.rommeluere@synchrotron-soleil.fr
† sonia.minolli@nexeya.com

CURRENT SITUATION

TANGO Device Server Concept

The TANGO system works around the concept of "Device Server ". A device server is a program that deals specifically with permanent dialogue ("server") with the apparatus ("device"). The PLCServer is a DS (written in C++) based on a PLC device.

Use of Client/Server Model

The PLCServer is the core of the data exchange mechanism between the SIEMENS 3XX series PLCs and the TANGO software bus. This DS is responsible for performing readings and writes from/to PLC data blocks via a dedicated protocol over TCP/IP and for distributing this data to its clients (see Fig 1).

Clients are higher-level DS. They represent physical equipment such as valves, pumps, gauges, etc. They communicate with the PLCServer via TANGO's internal protocol.

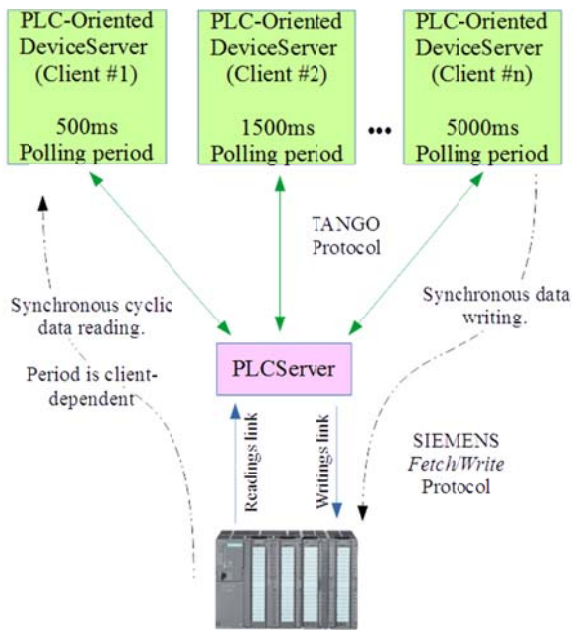

Figure 1: Communication model between Tango devices and PLC using PLCServer.

After registering with a PLCServer, clients cyclically address the PLCServer via a polling mechanism to retrieve a data area present in a DB of the target PLC.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA158

The DB number, offset and size of the data area, as well as the polling period are defined in the properties of the client. At each request, the PLCServer synchronously retrieves the requested data via the SIEMENS *Fetch* protocol and transmits it to the requesting client. The writes use the same type of request, via the *Write* protocol, except that they are not cyclical.

THE NEED TO EVOLUATE

Limits of the Current Model

The current PLCServer suffers from a performance loss problem when a significant number (typically a few dozen) of clients registers and makes cyclical read requests. The slow execution of Fetch communication sessions (which are serialized by the PLCServer) delays the refresh of the data in the client DS and even causes timeout if the reading frequency imposed by the client cannot be respected.

Several workarounds have been applied in recent years to push back the number of clients accepted by a PLCServer:

- Increase the polling period of clients to decrease the number of read requests per unit of time.
- Start multiple PLCServers communicating with the same physical PLC, but via different Fetch/Write links declared on separate TCP ports.
- Allow the main program of the PLC (named OB1) to run several empty cycles. Empirically, it was found that the CPU time released thus freed allowed the Ethernet communication to be more efficient.

However, all of these solutions generate operating or configuration constraints. They are unable to cope with the natural increase in the number of physical equipment, and therefore client DS which are linked to PLCs in production at SOLEIL.

Incompatibility with the New PLC SIEMENS Series

Since the mid-2010, SIEMENS has been marketing new PLC series (12XX, 15XX, LOGO) that do not support the *Fetch/Write* communication protocol. With the announcement of the end of the 3XX series PLCs' commercialization by 2022, SOLEIL must adapt its PLCServer if it wishes to be able to use the new PLC series via TANGO.

The reasons described above led SOLEIL to decide to provide a new, more efficient and perennial DS: the PLCServerV3.

Constraints of Evolution

The development of the PLCServerV3 is subject to several operational constraints. They are due to the fact that all the PLC configurations of SOLEIL (several hundred) cannot be modified in a time short enough to last within the duration of a machine shutdown and that some PLC must be kept in operational conditions almost all the time.

The PLCServerV3 was designed with these constraints in mind:

- No need to change client DS binaries or their properties.
- Requires only little change in the properties of PLCServer.
- No need to change the configuration of the current PLCs communication links.

The goal was to make the PLCServer version change almost transparent for programmers and PLC users whose applications, sometimes old, almost never evolve (and often do not need more communication performance).

For all these reasons, the development efforts of the PLCServerV3 almost exclusively focused the PLCServer/PLC communication layer, without affecting the methods of dialogue between the PLCServer and the clients.

Snap7, the S7 Communication Library for Ethernet

After a study phase of the different software solutions, the Snap7[3] library was chosen. The main characteristics that led to its selection are:

- It bases its communication on the *S7* protocol, which is the native and fastest communication protocol available on all SIEMENS PLCs. *S7* connections do not require PLC-side configuration. In addition, *S7* links can coexist with existing *Fetch/Write* links, allowing Snap7 to be used without interfering with the PLC's network configuration and leaving programmers with the choice of when to remove the obsolete *Fetch/Write* links.
- It is available as a C++ library that can be easily interfaced and recompiled with code already developed for the DS.
- It respects the PLCServer data request template. Snap7 is naturally able to read/write data as the PLCServer does, based on information such as DB number, offset and length of data requested by the clients.
- It is open source, distributed under Lesser General Public License version 3.0 (LGPLv3).
- It is very well documented and kept up to date by its author.

WHAT'S NEW IN PLCSERVERV3

Benefits of Snap7

Data aggregation

Snap7 has a function of aggregating data in the same exchange frame. To reduce the number of frames exchanged, the use of this function is preferred. The new PLCServer, known as PLCServerV3, implements an algorithm that groups together the data area to be in order to efficiently fill the frames (see Fig 2). It determines the number of user data area ('UsefulData') encapsulated in *S7* telegrams (themselves encapsulated in ISO telegrams and the TCP) according to the PDU parameter PDU (Pro-

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA158

tocol Data unit - 240 to 960 bytes depending on the type of PLC) which is negotiated during the connection.

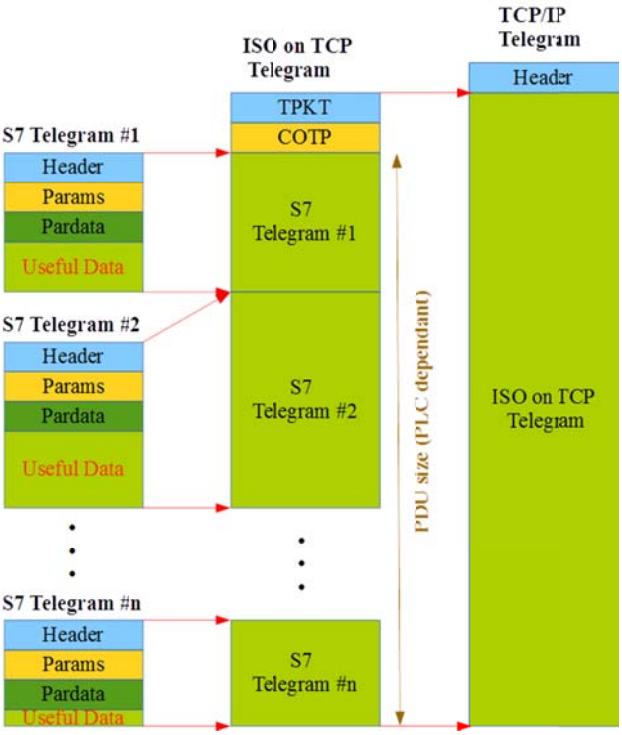

Figure 2: Protocol encapsulation and PDU filling optimization.

Communication test and system info functions

Snap7 embeds a simple ping troubleshoot function, used to perform basic communication test.

Snap7 also proposes functions to get CPU or communication module name, state, serial number and other information. Retrieving of ping response and system info is done by PLCServerV3 at very low frequency (typically every 10 seconds).

Other Enhancements of the PLCServerV3

Asynchronism and categorization of clients

In order to minimize the increase in network load when adding clients, an internal threading mechanism decouples exchanges with the PLC from exchanges with clients. The PLCServerV3 transmits data asynchronously between PLC and clients.

Clients who register with PLCServerV3 are classified according to their polling period into two categories:

- The SLOW category if their polling period is greater than a 'SlowPollingPeriod' (SPP) variable defined in the PLCServerV3 properties.
- The FAST category otherwise, combined with a 'FastPollingPeriod' (FPP).

In operation, clients query the PLCServerV3 with their polling period, but the data is only read from the PLC with the FPP and SPP periods.

When the PLCServer starts up, two *S7* links are established for the readings, one per category of clients. The writings from the clients (less frequent and non-periodic) are transmitted synchronously via a third link (see Fig 3).

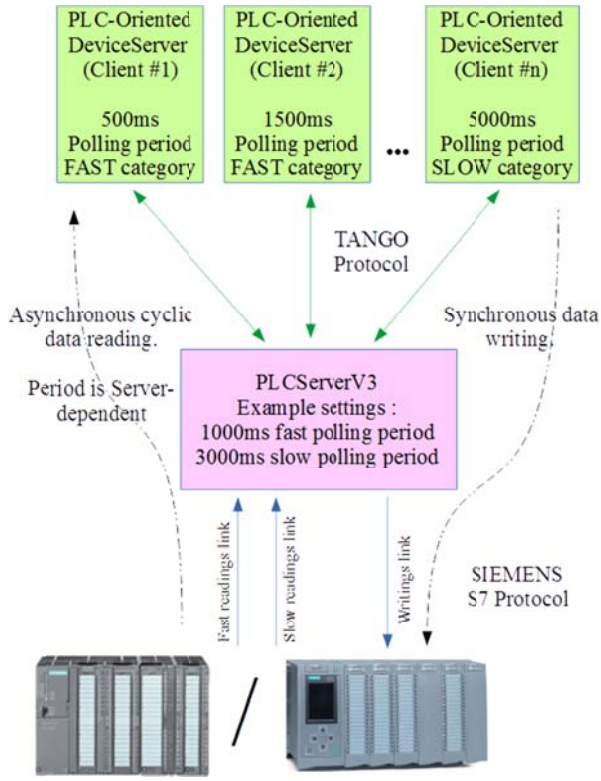

Figure 3: Communication model between Tango devices and PLC using PLCServerV3.

A cache mechanism allows the PLCServerV3 to respond to the clients between two *S7* readings without causing timeout even in case of high demand. If the *S7* data cannot be acquired with the FPP and SPP periods, an exception is sent to clients to alert them of overload or communication loss.

Other attributes, such as the rates of the data transiting the PLCServerV3, have been added to easily estimate the operating state (see Fig 4).

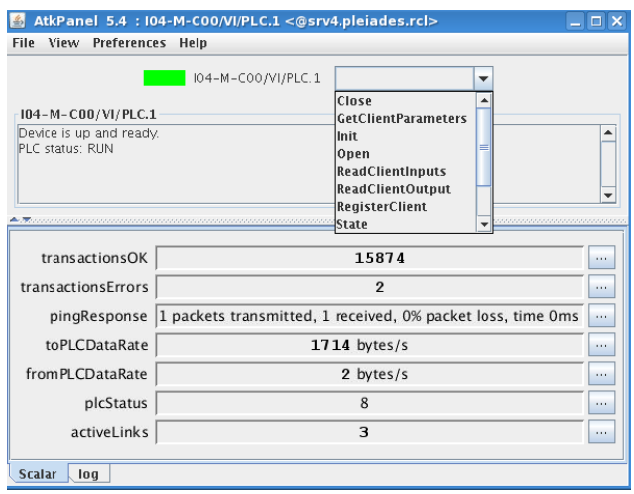

Figure 4: State, status, commands and attributes view of PLCServerV3 in operation.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA158

Table 1: Summary of PLCServers features

Item	PLCServer	PLCServerV3
Link type	*Fetch/Write* Must be declared	*S7* No configuration needed
Number of links	2 or 4	3 minimum
Data reading polling	Synchronous. Period is client dependent	Asynchronous Clients are classified according to their polling period into two categories.
Suitable for 3XX PLC series	Yes	Yes
Suitable for 15XX PLC series	No	Yes

PERFORMANCES, LIMITATIONS AND BUGS

Performances

The main performance sought is that which allows the PLCServerV3 to read data DBs at a frequency equal to or greater than that of data recovery by clients.
Table 2 shows the data rates reached for different DB numbers and sizes, after maximum reduction of the PLCServer reading periods (FPP and/or SPP). These tests were performed in real conditions (i.e. the target PLC is executing a real program and the communication is performed through on a switched network shared with other devices).

Table 2: Performances

Criteria	CPU315-2DP + CP343	CPU1516-3 PN/DP
Data Rate for a single DB	12.1 KB/s for 2000 32-bit reals with FPP=660 ms	630 KB/s for 15900 reals with FPP=100 ms
Data Rate for large number of DBs (Between 10 and 40 Bytes)	2.6 KB/s for 73 clients with FPP=1700 ms plus 40 clients with SPP=5000 ms	Not tested

Limitations

SPP and FPP limits values
The sum of the reading times of the clients DBs of the same category limits the minimum size of FPP and SPP because the readings are serialized by the PLCServer. This will be improved by spreading the readings over a larger number of *S7* links (applicable only to new PLC series).

Optimized block incompatibility for 15XX PLC series
SIEMENS new PLC series offers the possibility to use DB with optimized access. These DB do not have a specifically defined structure. The data elements receive only one symbolic name in the declaration and no fixed address in the block. Since Snap7's data request model requires explicitly offset and data length information, it is mandatory to turn off the optimized block access feature in new PLC series.

Known Bugs

A random bug still interferes with the long-term stability of the PLCServerV3. It is infrequent (every 5 hours or so). It manifests itself by a data reception error, then timeout and unrecoverable TCP error. While the search for the cause continues, a workaround is applied. It consists in restarting the connection automatically if this bug occurs.

CONCLUSION

With the PLCServerV3, SOLEIL has a replacement for its current software. It is more efficient and it permits an easy deployment which does not require intervention on PLCs or clients DS in production (see Table 1). It is likely to be installed on a widespread basis in 2018. It is compatible with the new PLC SIEMENS series which could serve as the standard in the future, for SOLEIL and for other institutes using TANGO.
The first stage of the roadmap is fulfilled. This will be followed by the definition of a strategy to address Operational Readiness (progressive replacement of the existing install base or maintenance of production configurations up to a long shutdown of the accelerators for major upgrade) as well as the adaptation of the operational organization to the new equipment.

ACKNOWLEDGEMENT

The PLCServerV3 was tested and used on the 'factory of the future' demonstration platform of CEAtech[4] implanted within the Peugeot/Citroen plant of Trémery, introducing TANGO in an industrial environment.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA158

REFERENCES

[1] French synchrotron light facility, https://www.synchrotron-soleil.fr

[2] Software toolkit for distributed control systems, supervisory and data acquisition, http://www.tango-controls.org

[3] Snap7, http://www.snap7.sourceforge.net

[4] French industry innovation accelerator, http://www.cea-tech.fr/cea-tech/english/Pages/home-uk.aspx