ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

LTE/3G-BASED WIRELESS COMMUNICATIONS FOR REMOTE CONTROL AND MONITORING OF PLC-CONTROLLED MOBILE VACUUM DEVICES

R. Ferreira, S. Blanchard, P. Gomes, G. Pigny, CERN, Geneva, Switzerland
T. Fernandes, Polytechnic of Leiria, Leiria, Portugal

Abstract

All particle accelerators and most experiments at CERN require high (HV) or ultra-high (UHV) vacuum levels. Contributing to vacuum production are two types of mobile devices: Turbo-Molecular Pumping Groups and Bakeout Racks. During accelerator stops, these PLC-controlled devices are temporarily installed in the tunnels and integrated in the Vacuum SCADA, through wired Profibus-DP. This method, though functional, poses certain issues which a wireless solution would greatly mitigate. The CERN private LTE/3G network is available in the accelerators through a leaky-feeder antenna cable which spans the whole length of the tunnels. This paper describes the conception and implementation of an LTE/3G-based modular communication system for PLC-controlled vacuum mobile devices. It details the hardware and software architecture of the system and lays the foundation of a solution that can be easily adapted to systems other than vacuum.

INTRODUCTION

The extensive network of particle accelerators and experiments at CERN, the European Centre for Nuclear Research [1], features the largest operational vacuum system in the world [2]. These accelerators, represented in Figure 1, have extremely strict pressure requirements.

In order to minimize the interaction between the particle beam and any residual air molecules, pressure in the beam pipes must be kept below 10^{-10} mbar (UHV). The superconductive magnets and RF cavities in the LHC, together with the helium distribution lines, require vacuum for thermal insulation of the associated cryogenic system. This is typically maintained between 10^{-6} and 10^{-8} mbar (HV). Such low-pressure levels are created and maintained using a wide array of methods and technologies.

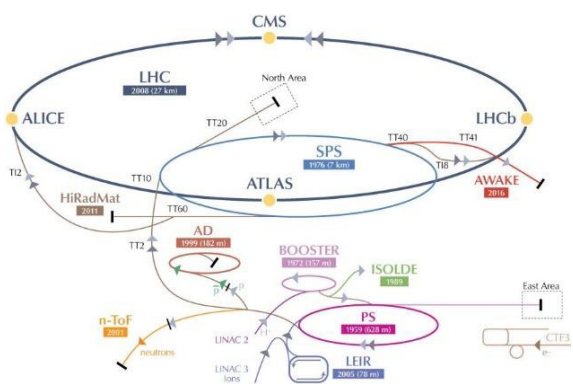

Figure 1: The CERN Accelerator Complex.

These include turbo-molecular pumping, baking of the vacuum vessels, and techniques such as NEG, ionic, cryogenic and sublimation pumping [3] [4]. Most of the equipment required to create and maintain HV and UHV is permanently fixed in place.

Several hundred pumping groups are installed throughout all accelerators in the complex, for both beam and insulation vacuum purposes. The same can be said for NEG, ionic, cryogenic and sublimation pumps, which can be found by the hundreds in most of the accelerators. In several sections, the inside of the beam pipes is actually coated with a NEG, which essentially acts as a pump by adsorbing molecules. In others, the pipes are cryogenically cooled in order to condense certain gases on their walls, further reducing pressure.

Though most of this is achieved with fixed equipment, two types of mobile devices contribute to the creation and management of vacuum: Turbo-Molecular Pumping Groups (VPGMs) and Bakeout Racks. VPGMs (Figure 2) are trolley-mounted pumping groups, containing one primary rotary-vane pump and one turbo-molecular pump, along with all required valves and some additional equipment. These PLC-controlled groups are temporarily installed at necessary locations, to either perform the initial pump down from atmospheric pressure (the LHC, for example, has no fixed pumping groups on the beam pipe) or to complement the other pumping methods.

Figure 2: Turbo-Molecular Pumping Group.

Bakeout Racks (Figure 3) also play a major role in reaching low pressures. Prior to accelerator operation, the beam pipes and several elements of the vacuum system are baked, by being heated to temperatures in excess of 200ºC for over 24 hours. Baking these vacuum vessels evaporates molecules that may have condensed on their inner walls

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

and also activates the NEG coatings, where existing. This process is fully managed by the Bakeout Racks, which are also PLC controlled.

Figure 3: Bakeout Rack.

The control and monitoring of such a massive system is not a trivial matter. The Vacuum Control System is a PLC-based distributed industrial control system which makes extensive use of Siemens technologies [5]. If we take into account the whole accelerator complex, over 200 S7-400 and S7-300 PLCs are permanently installed. In mobile devices we find S7-200 and S7-300 CPUs, totalling around 400 mobile PLCs. The S7-1500 and S7-1200 models have started to be deployed in both fixed and mobile situations.

The SCADA applications for the three main accelerator complexes, along with several smaller applications, are implemented with Siemens WinCC-OA, heavily customized for our purposes.

Mobile devices, once installed and connected to the control system, must be temporarily integrated in the Vacuum SCADA for remote control and monitoring. Currently this is achieved through Profibus-DP, using network cables that are permanently installed in place (this method is described in detail in the next section). The goal of the project – and subject of this paper – is the development of an alternative, wireless method to integrate these mobile devices in the vacuum control system.

PROFIBUS-DP MOBILE INTEGRATION

At this time the integration of mobile devices in the SCADA using Profibus networks exists only on the LHC, LINAC4, and a couple of the newer installations. Let us for now consider the case of the LHC, as the implementation in the remaining machines is essentially a downscaled version of the same thing.

General LHC Layout

The LHC is housed in a 27 Km long underground circular tunnel. Along its length are 8 roughly equidistant "caverns" (P1 to P8 in Figure 4), where most control equipment is installed. In between these 8 main caverns we also have some 20 smaller "alcoves" with additional equipment.

In each of these points we have Siemens S7-400 PLCs which, among other roles, act as Master controllers for the mobile Profibus system.

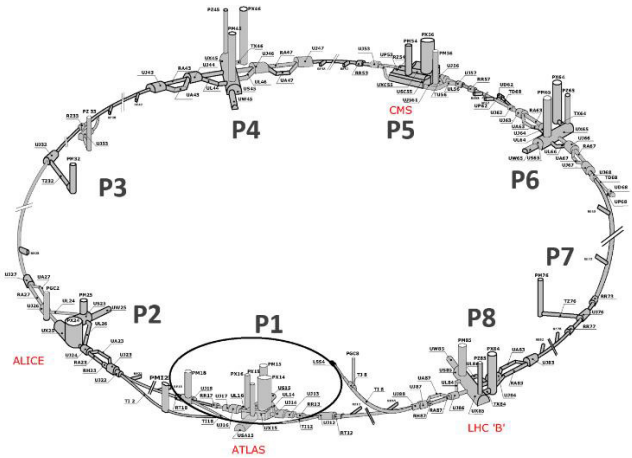

Figure 4: The Large Hadron Collider structure.

There are typically two Master PLCs per cavern and one per alcove. From each alcove, as there is a single PLC, there is one Profibus cable segment to the left and one to the right. In the case of the caverns, one PLC manages the equipment installed to the left side and the other to the right. A Profibus cable is sent from each PLC to the respective side of the tunnel. Full coverage of all necessary areas of the LHC tunnel is achieved with around 30 PLCs managing an equal number of Profibus-DP networks.

Each network segment in the tunnel is around 600m. Mobile devices can be connected in two ways, depending on the location. In some areas the Profibus cable has a large number of pre-installed connectors where the devices can be directly plugged in. In others the network is periodically interrupted by link boxes with input and output connectors, so that complete network loops with several devices might be installed. If nothing is connected, the box must be shunted in order not to break continuity (Figure 5).

Figure 5: Profibus link box.

During technical stops, vacuum operators install the mobile devices at required locations and specify their position using the touch screen. Bakeout Racks are identified by sector name and occurrence number (there might be several racks per sector). VPGMs are identified by the name of the flange they were connected to. Operators then connect them to the Profibus network using an available flying connector or by creating a new network loop with the link boxes.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

Software Infrastructure

The mobile Profibus network in each Master PLC is preconfigured with addresses for the mobile devices. Addresses 3 through 67 are reserved for the Siemens EM277 module (which provides Profibus connectivity in the S7-200 based VPGMs). Addresses 68 through 125 are configured for the CP-342-5 module, which is used on the Bakeout Racks as a Slave DP module. Whenever a Bakeout Rack or VPGM is connected to the network, the Slave device with the corresponding address becomes available and the Master initiates the SCADA registration procedure. This process is rather complex and includes multiple checks and handshakes, but can be described in a simplified way as follows:

1. Master requests TypeID from Slave (there are multiple models of VPGMs and Bakeout Racks).
2. Master transmits TypeID to SCADA.
3. If TypeID is valid, an initial handshake between Master and Slave is performed.
4. Existing resources on the Master (Data Blocks) and SCADA (Data Points) are reserved for the device, according to its type.
5. Master requests the location of Slave (which was input by the operator upon installation) and transmits it to the SCADA.
6. SCADA verifies the validity and availability (occupied or not) of that position. If everything is OK an acknowledgement is sent to the Master, which relays it to the Slave.
7. The registration process is now complete and data exchange may proceed.

After successful completion of this process the mobile device becomes visible in the SCADA. VPGMs are shown directly in the synoptic, in their actual location, while Bakeout Racks are listed according to sector in a dedicated panel. The SCADA cyclically requests the state of each mobile device through the Master, which relays the request to the slave. The same occurs with commands.

If the device is disconnected it gets automatically unregistered after a given delay. The associated resources on the SCADA and PLC are released and the device disappears from the system.

Issues

The mobile Profibus system has been in operation for several years, serving its purpose as expected. It is well engineered and has proved to be mostly reliable. Some issues and shortcomings are, however, apparent:

- The operators who install the mobile devices are not control nor fieldbus experts. They often create issues which can bring the whole network segment down. These include star topologies, illegal loops, missing shunts on the link boxes, or missing network terminations.
- The repetitive manipulation of the Profibus cables and connectors causes accelerated deterioration of the material (Figure 6).

Figure 6: Deteriorated cable in a Profibus connector.

- There are only 124 useable Profibus addresses for Profibus slaves. As we have over 400 mobile devices, some addresses have to be repeated. Sometimes, by mistake, two devices with the same address end up in the same network, causing problems in the whole segment.
- Connectivity is not available in the whole accelerator complex. Cabling all the tunnels and experiments with a Profibus network would be considerably expensive.

These issues, as we will see, can be almost completely addressed with a wireless system.

WIRELESS TECHNOLOGIES

There are two main reasons why a 3G/LTE-based solution was chosen over standard 802.11b/g/n wireless or other wireless protocols: the cost of implementation and the challenging conditions in the tunnels during operation.

Particle accelerators produce two kinds of ionizing radiation: synchrotron radiation (high-energy photons emitted by charged particles circulating around a ring) and radiation due to the interaction between stray particles from the beam and elements of the accelerator such as the walls of the beam pipe or the collimators. Non radiation-hardened electronics cannot be present in the tunnels during operation because they would be quickly destroyed by the radioactive environment. This means that wireless access points could not be permanently installed in the tunnels and would have to be brought in for every intervention (and interfaced with the rest of the network). This is simply not feasible in the case of technical stops of a few days (or hours). We could consider installing the access points in shielded areas and placing only the antennas in the tunnels, but it would be hard to financially justify the installation of hardware to cover nearly 40 Km of tunnels just to support a single project.

There is, however, mobile cell coverage in all accelerator tunnels. 3G is available in all areas, LTE in an increasing number of them. This is achieved with leaky feeder-type antennas (essentially radiating cables) which are installed along the whole length of the tunnels, while the active electronics are kept in radiation-shielded areas.

The network is provided by Swisscom, although the APN (Access Point Name, the gateway between the mobile network and the CERN campus network) is managed by

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

CERN and taps directly in the CERN network infrastructure. From a security standpoint this is an extremely important detail, because it means that data flowing through the APN never leaves the CERN network and is never sent over the Internet.

This 3G/LTE network is therefore ideal for our application. There is already full coverage in all the accelerators and all the infrastructure is in place, meaning that there are no added costs to account for (apart from the modules on the PLC). There is, however, an operational cost associated with each SIM card (10 CHF/month) which somewhat conditioned our implementation, as shall be described.

3G/LTE Connectivity on PLCs

All models of Bakeout Racks are driven by S7-300 CPUs. Some have a recent CPU with an Ethernet interface, while in others Ethernet is provided by a dedicated module. VPGMs are controlled by the legacy S7-200 PLC, for which there is no way to reliably provide Ethernet connectivity without going in a fairly complicated and non-standard direction. These VPGMs are in the process of being updated with a new S7-1200 based control system, so we decided to focus solely on this new model. All S7-1200 CPUs provide by default at least one Ethernet port.

Siemens provides S7-1200 compatible modules for native mobile connectivity (the CP 1242-7 for GPRS and the CP 1243-7 for 3G/LTE). No such possibility exists for S7-300, so wireless communication must be performed over the Ethernet interface using a 3G/LTE router. We have opted for the SCALANCE M874-3, a small industrial 3G modem/router proposed by Siemens (Figure 7).

Figure 7: SCALANCE M874-3 3G Modem/Router.

Because we wish to have the same exact implementation for VPGMs and Bakeout racks, we opted to use the SCALANCE router for both. The point is to have a modular solution: whenever wireless connectivity is required on a mobile device the router is simply plugged to the device's Ethernet port and powered directly from the control crate. The network configuration will be explained later.

This modular approach also works as a cost saving measure. Tough we have several hundred bakeout racks and mobile pumping groups, there are rarely more than a few dozen in simultaneous operation. This means that we can simply have a reduced stock of 3G routers (and respective SIM cards) in storage and temporarily install them in whatever mobile devices require them. SIM cards may also be temporarily disabled if no interventions are expected, in which case the monthly fee will not be billed.

NETWORK ARCHITECTURE

The broad network architecture of the system is shown in Figure 8. There are two networks in the CERN campus and accelerator complex: the General Purpose Network (GPN) and the Technical Network (TN). GPN is the standard office network, connected to the Internet and addressable from outside the campus. TN is a dedicated internal network for the accelerators and experiments, disconnected from the Internet and only accessible from the GPN through designated gateway machines. All control devices, including PLCs and SCADA servers, are on TN, as are all elements of our wireless communication system.

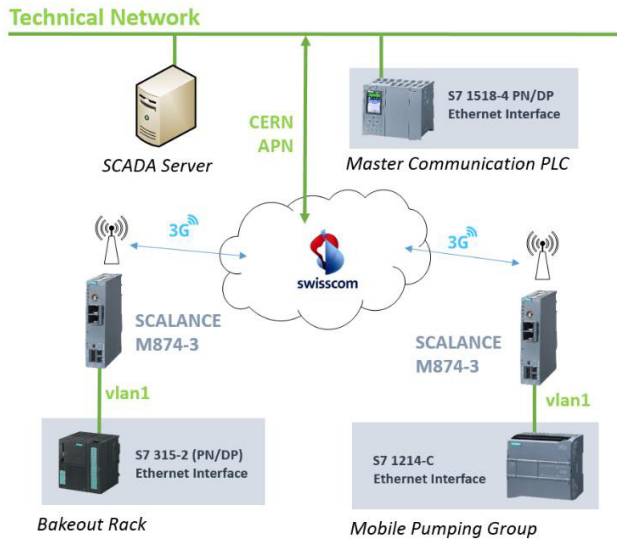

Figure 8: Network Architecture.

Each SCALANCE router has its own SIM card which is configured to access the data network through the CERN APN. These cards have been configured to receive, from the APN, fixed IP addresses that are fully routable over the TN but not accessible through the GPN nor over the Internet. This means that the routers are directly reachable by the Master Communication PLC on TN (refer to Figure 8).

Configuration

The purpose of the SCALANCE router is essentially to connect two networks: the internal LANs where the Slave PLC is connected (vlan1 on Figure 8) and the mobile 3G network. On vlan1 all routers have been given the fixed local IP *192.168.0.1*. Likewise, all slave PLCs on the mobile devices have been assigned IP address *192.168.0.2*. The routers were then configured to route all required traffic to and from the PLCs using these fixed IPs.

Inbound traffic is handled with port forwarding. All network traffic for ports 102 and 2424 coming in the 3G interface of the router gets routed to IP *192.168.0.2* (the PLC). Port 102 is used by the S7 Communication Protocol, and is routed so that we can directly access the PLC for diagnostics or reprogramming. Port 2424 is the one we use for the TCP connection between Master and Slaves.

Outbound traffic gets remapped by the router using NAT (Network Address Translation). The principle of NAT is illustrated in Figure 9. The Slave PLC (192.168.0.2) is sending a packet to the Master (137.138.245.130), which sends another in response. In the grey boxes the source and destination addresses of the packages are shown. In black

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

are the headers that NAT modified. When the Slave sends a packet to the Master, the router changes the source address so that the package appears to come from the outgoing interface of the router.

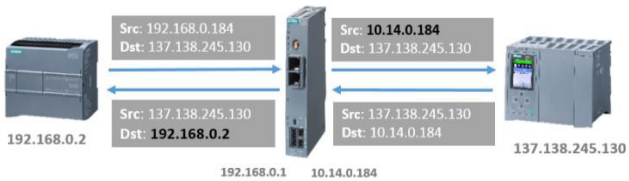

Figure 9: NAT Example.

The response from the Master arrives on the router addressed with the router's 3G IP; the router changes the destination address to the local IP of the Slave PLC, and delivers it on the internal network. It is important to note that the 3G interface of the router and the Master PLC are not on the same network. Between them there is further package routing happening, which is not shown on the figure.

Using NAT and Port Forwarding, the Slave PLCs are fully addressable on ports 102 and 2424, using the IP address of the SIM card of their respective routers. Direct access is possible from the Technical Network, using either the S7 protocol (for Simatic Pro / TIA Portal or SCADA communication) or TCP/UDP on port 2424.

Open User Communication

Data exchange between PLCs is implemented using the set of Open User Communication (OUC) blocks provided by Siemens [6]. OUC allows the establishment of IP connections between a PLC and any Ethernet capable partner. Both connection-oriented (TCP/IP, ISO) and connectionless (UDP) protocols are possible, depending on how the blocks are configured. Furthermore, connections are fully created and managed during runtime, so there is no need to previously configure them in the Hardware Configuration of the PLC, as is the case for S7 connections. The *TCON* and *TDISCON* Standard Library functions are used to create and disconnect the link, while data is transferred with the *TSEND* and *TRCV* blocks.

For our particular implementation we establish between the Master and Slave PLCs a TCP/IP connection on port 2424. The Slaves are permanently listening on this port and the Master acts as the Active partner, taking the initiative to establish the connection. Once the link is up, a dedicated protocol – described next - takes over.

COMMUNICATION PROTOCOL

The whole process, including the registration of mobile devices and subsequent cyclic data exchange, is managed by the Master PLC, a Siemens S7-1518/4; it supports a maximum of 192 connections via its integrated interfaces, more than enough for our application. The SCADA Server communicates only with the Master PLC and never directly with the slave devices. Contrary to what currently happens in the Profibus based system, the SCADA is not involved in the registration or data exchange with the mobile devices, it simply reads the data made available by the Master and relays commands through it (Figure 10). A dedicated protocol was developed to handle the whole process.

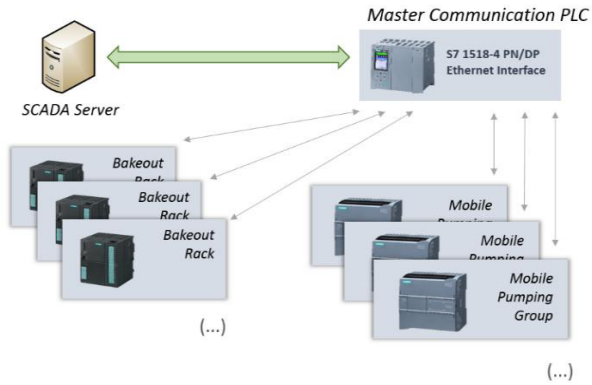

Figure 10: SCADA/Master/Slave Communication Scheme.

Protocol Data Unit Structure

The Master and Slave exchange data packets of a fixed structure. The protocol uses a 138 byte long Protocol Data Unit (PDU), with a 10 byte header for control data and a 128 byte data payload. The PDU is nearly identical in both directions, and its structure is show in Table 1.

Table 1: PDU Structure (Offset Value in Bytes)

Offset	Master to Slave	Slave to Master
0.0	Type ID	Type ID
2.0	Connection State	Connection State
4.0	Connection ID	Connection ID
6.0	Request Code	Response Code
8.0	Page Number	Page Number
10.0	Request Data	Response Data
…		
137.0		

Type ID identifies the device sending the packet. The Master PLC is always type 255, while the different models of Pumping Groups and Bakeout Racks have type codes in the range 1 – 254.

Connection State identifies the current state of the connection. It is calculated by the Master and sent to the Slave, which includes it in all subsequent data exchanges. The values are as follows:

- **0** [*Disconnected*] – The Slave is unreachable or a TCP connection has not been established yet.
- **1** [*Connected*] – The Slave is reachable over the network. A TCP connection has been established.
- **2** [*Recognized*] – The Slave has correctly received and returned the handshake number sent by the Master (*Connection ID*). It has also supplied its own name, identifying itself to the Master.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

- **3** [*Ready*] – The Slave has supplied a valid (existing and unoccupied) location to the Master. The Master has registered it to that location. Data exchange is ongoing.

Connection ID identifies each particular TCP/IP connection on the Master. The value is decided by the Master and sent to the Slave as a handshake value, to be included and all subsequent packets.

Page Number is used only for Bakeout Racks. Because their full state data is larger than the *Response Data* area, it is spread over several 128 byte pages, which are individually requested.

The *Request* and *Response Codes* identify the purpose of each packet:

Table 2: Request and Response Codes

Code	Request	Response
1	Send Handshake and Request Type ID	Return Handshake and Type ID
2	Request Device Name	Return Device Name
3	Request Device Position	Return Device Position
4	Request Occurrence Number	Return Occurrence Number
5	Request Device Data	Return Device Data
6	Send Device Commands	Confirm Device Commands

The *Handshake (Connection ID)* and *TypeID* are sent and returned in the header of the PDU. *Device Name* and *Position* are returned as Strings in the *Response Data* area. The *Occurrence Number* is sent as an Integer in the *Response Data area* as well. *Device Data* is the state of the mobile device and *Device Commands* are the orders sent to it, both packed in a predefined binary format. *Data* is returned by the Slave in *Response Data* and *Commands* are sent by the Master in *Request Data.*

Software Architecture

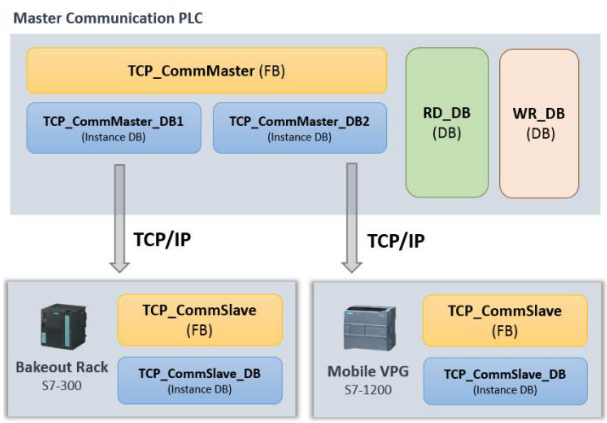

Figure 11: Software Architecture.

Figure 11 shows the simplified software architecture of the system. On the Master side, the protocol code is implemented in Function Block (FB) *TCP_CommMaster*. One instance of this block is required per SIM card and identified by its IP address. The Master PLC will have as many instances of *TCP_CommMaster* as SIM cards deployed, each one processed independently. These instances exchange data with the RD_DB and WR_DB Data Blocks, which are the ones actually accessed by the SCADA.

On the Slave PLCs, the system is managed by the FB *TCP_CommSlave*, of which there is a single Instance DB per PLC. This DB contains the information about the Type and name of the Slave.

These two Function Blocks essentially implement the State Machines that run the whole protocol.

State Machines

Two different State Machines (Master and Slave) govern the registration and automatic data exchange process. These are fairly long and too complex to reproduce here in detail; a very simplified version of the registration process from the point of view of the Master is shown in Figure 12.

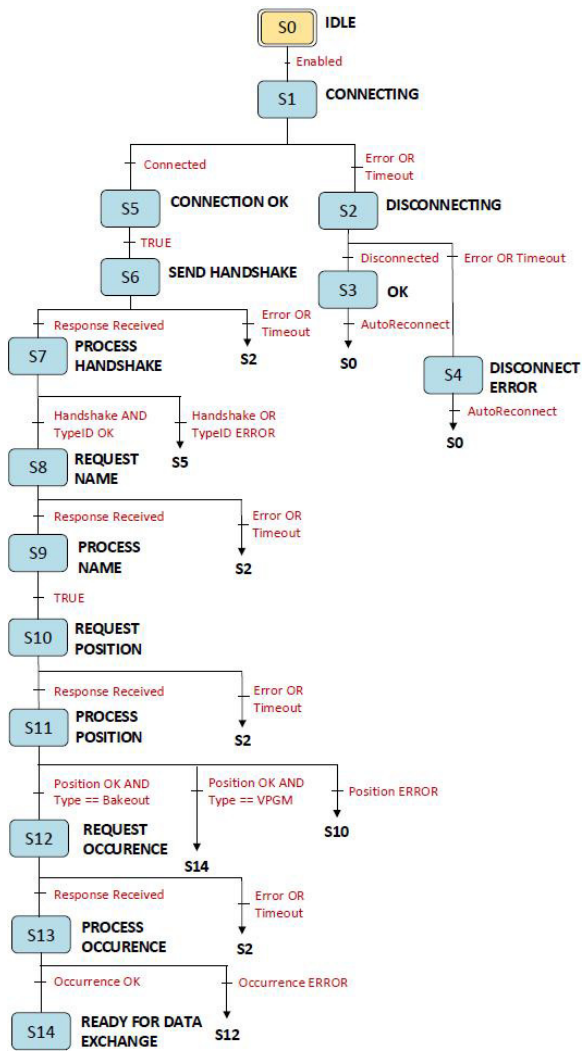

Figure 12: Slave Registration Process.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-MOCPL04

This figure is not meant to represent the actual implementation of the state machine, but rather the steps involved in the automatic registration of Slave devices.

Once the Ready state has been reached, the Master starts cyclically requesting data from the Slave. Any commands sent from the SCADA are also relayed to the Slave by the Master.

SECURITY

Cyber security is, of course, a prime concern for any remotely accessible Industrial Control System. In our particular case, because the system is completely integrated in CERN's network infrastructure, this issue is centrally addressed by the organization's security practices [7]. Access to the Technical Network is tightly controlled and constantly monitored, and care was taken to guarantee that all network traffic is kept inside it. Data is routed from the APN directly to TN, and no SIM card is visible from the GPN or any other external network, nor addressable over the Internet.

If this were not the case (or if the system were to be implemented in a different infrastructure), extra precautions would have to be taken. The use of VPN tunnels, for example, would be strongly recommended. The SCALANCE M874 router supports it, but extra hardware is required to implement the VPNs. Siemens provides dedicated security modules - such as the SCALANCE S612 - which feature integrated firewalls and other features. For a secure implementation using public or unsecured networks an in-depth study would need to be conducted.

CONCLUSION

A 3G/LTE-based wireless communication system for PLC to PLC data exchange has been designed and implemented. Standard industrial networking hardware and technologies have been employed, without the need for dedicated hardware development. A dedicated protocol to support the operation of mobile Bakeout Racks and Pumping Groups has also been implemented. The main shortcomings of our current Profibus solution have been addressed:

- The integration of mobile devices in the SCADA is now possible in every accelerator and experiment, without the need to install a new cabled infrastructure.
- The operators are not required to handle any cables or connectors, thus avoiding degradation of material.
- Being wireless, there is no chance that a topology error or missing shunt affects the whole network and all devices on it.
- The address space is increased from 124 possible Profibus addresses to the full range of free IP addresses on any particular subnetwork.
- The APN automatically distributes fixed IP addresses to the SIM cards, so address conflicts will not occur.

The system was designed as a full alternative to our current Profibus-based method. Both its architecture and protocol can be easily adapted to other situations and systems.

Tests have been performed on the LHC tunnel, shown in Figure 13. The Master PLC was installed in our automation lab, on the surface, while a Slave PLC on a trolley with a UPS was moved around the LHC for about 1 Km, spanning several mobile cells. The connection and data exchange process held steady for the full duration of the test, which took roughly one hour.

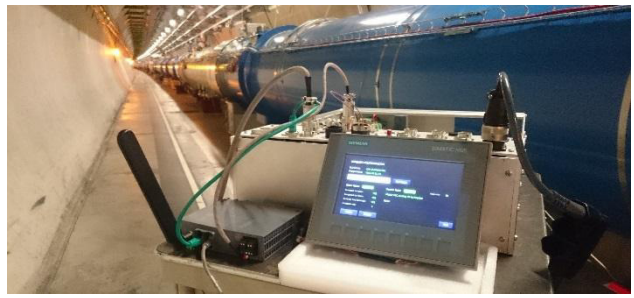

Figure 13: Ongoing tests on the LHC tunnel using a VPGM crate.

The SCADA developments, required to show the mobile devices on the synoptic and to provide dedicated panels for monitoring and control, are currently under way. They are, however, outside the scope of this paper.

ACKNOWLEDGEMENT

The authors wish to thank Filipe Salgueiro and André Ramos, students from the Polytechnic Institute of Leiria, for their valuable work in evaluating the capabilities of the various Siemens communication modules and their study of possible network architectures.

REFERENCES

[1] The CERN Accelerator Complex, http://home.web.cern.ch/about/accelerators

[2] A Vacuum as Empty as Interstellar Space http://home.cern/about/engineering/vacuum-empty-interstellar-space

[3] J. M. Jimenez, "LHC: The world's largest Vacuum Systems being commissioned at CERN", in *Proc. European Particle Accelerator Conference. (EPAC'08)*, Genoa, Italy, 2008, pp. 1959-1961.

[4] J. M. Jimenez, "LHC Vacuum Upgrade During LS1", in *2012 Workshop on LHC Performance*, Chamonix, France, Feb. 2012, pp. 230-235.

[5] P. Gomes *et al*., "The Control System of CERN Accelerators Vacuum," in Proc. *International Conference on Accelerator and Large Experimental Physics Control Systems 2011. (ICALECPS'11)*, Grenoble, France, Oct 2011, pp. 354-357.

[6] *Open TCP/IP Communication via Industrial Internet,* Siemens Simatic, Manual, Edition 12/2005.

[7] S. Lüders, "Update on the CERN Computing and Network Infrastructures for Controls (CNIC)," in *Proc. International Conference on Accelerator and Large Experimental Physics Control Systems 2007, (ICALECPS'07)*, Knoxville, Tennessee, USA, 2007, pp. 472-474.