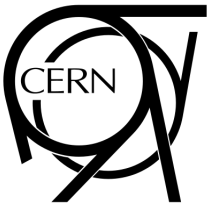
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Industrial Automation

Dr. Yvonne-Anne Pignolet

Dr. Jean-Charles Tournier

CERN Data Center Case Study



Group B
Yann Dupont-Costedoat
Augustin Christensen
Lucas Prado Sendagorta
Andrea Sestini

Spring semester 2017

Contents

1 Introduction

1.1 Problem statement

The CERN (*Conseil européen pour la recherche nucléaire*) is a European research organization located close to Geneva (Switzerland/France) that operates the largest particle physics laboratory in the world. Many experiments are held yearly, and perhaps the most famous one is the LHC experiment, which aims at proving the existence of the Higgs Boson. This experiment alone produces 30 petabytes of data per year, while it is estimated that the CERN stores 130 petabytes of data on a normal basis. Those number are ridiculously high: 10'000 servers working 24/7 are necessary just for the functioning of this organization. Also, a remote extension of the data center is hosted at the Wigner Research Center for Physics in Hungary, which is connected to the main CERN campus through two independent and dedicated 100Gb/s fibre optic lines.

For all this mass of data to be processed, a huge energy consumption from servers is required, which will at the same time produce huge quantities of heat. Therefore the cooling and ventilation system is crucial for the good functioning of the data center and the CERN itself.

We have been contacted in order to implement the control system of the cooling infrastructure for the CERN data centers, in both Switzerland and Hungary. This will include the system architecture, the choice of hardware/software, the communication protocols... Also, we were asked to integrate the supervision system with a TANGO control system. Last but not least, a security analysis and a cost estimation will be realized in order for the client to be fully aware of the implications of such a control system.

1.2 Specifications & Assumptions

Instructions for our work were vague, so we have very few specifications to keep on with. Following is a list of the information we have:

- The data center includes 10'000 servers hosted in 3 rooms running 24/7
- The data center includes an extension, situated in Hungary and connected through two independent and dedicated 100Gb/s fiber optic lines.
- The cooling and ventilation of the computing rooms is done through cold air introduced in the building via big pipes coming from the roof and going down to the floor.
- Three chillers on the building roof are responsible for pushing down the air, therefore three fans are to be taken into account.

We are going to make some assumptions in order to reduce the scope of our analysis. Those assumptions will be as realistic as possible, and will be previously accepted by two control systems experts in their respective domain, Dr. Yvonne-Anne Pignolet and Dr. Jean-Charles Tournier. Here are the assumptions that will be necessary for the following parts of our work:

- The project is time constrained.
- The main focus is the cooling system and not any other part of the site such as the control of the servers.
- Two different data centers are to be taken into account, each with three roof fans and a different quantity of servers (as explained later on). *We are only going to describe one of the two since the systems will be identical*

2 Work distribution

Our team is composed of four members, of various nationalities and coming from different backgrounds. We decided to split the workload based on those differences, and trying to optimize as much as possible the usage of the strengths of each member.

(a) Andrea Sestini
Génie Mécanique, Italian
Focused on sections 3, 4, 7 with Lucas

(b) Lucas Prado Sendagorta
Génie Eléctrique, Spanish
Focused on sections 3, 4, 7 with Andrea

(c) Augustin Christensen
Génie Eléctrique, French
Focused on sections 5, 6, 7 with Yann

(d) Yann Dupont
Génie Informatique, French
Focused on sections 5, 6, 7 with Augustin

Figure 1: Team members and work repartition

This task division does not mean that each team member did not help in any other part of the project. In order to complete the project on time, a high level of team work and collective exchange of opinions was necessary.

3 Overall system architecture

Data centers must stay within certain temperature and humidity ranges to function optimally and to prevent hardware failure. If the temperature rises too high, gear will begin to malfunction or become damaged. Internal components begin to swell and pull away from each other (or simply burn-up). A data center will want to keep a controlled temperature range of 18-27 °C. This is well within ASHRAE's (American Society of Heating, Refrigeration, and Air-Conditioning Engineers) guidelines for data processing environments, as shown in Figure2.

Class	Equipment Environment Specifications									
	Product Operation [a, b]							Product Power Off [b, c]		
	Dry Bulb Temperature (°C)		Humidity Range, Non Condensing		Maximum Dew Point (°C)	Maximum Elevation (m)	Maximum Rate of Change (°C/h)	Dry-Bulb Temperature (°C)	Relative Humidity (%)	Maximum Dew Point (°C)
	Allowable	Recommended	Allowable (% RH)	Recommended						
1	15 to 32 [d]	18 to 27 [e]	20 to 80	5.5°C DP to 60% RH and 15°C DP	17	3050	5/20 [f]	5 to 45	8 to 80	27
2	10 to 35 [d]	18 to 27 [e]	20 to 80	5.5°C DP to 60% RH and 15°C DP	21	3050	5/20 [f]	5 to 45	8 to 80	27
3	5 to 35 [d, g]	NA	8 to 80	NA	28	3050	NA	5 to 45	8 to 80	29
4	5 to 40 [d, g]	NA	8 to 80	NA	28	3050	NA	5 to 45	8 to 80	29

Figure 2: ASHRAE's guidelines for Data Centers

Humidity must also be watched to ensure all gear work in the data center. If the air in the data center is too humid, water may condense on the internal components, resulting in shorts. If the air is too dry, a data center risks static build up, which can also result in electrical shorts. Typically, a data center will also want to maintain its humidity concentration within the 20-80% range. At any rate, cooling and environmental control is very important. If any part of the data center were to fail, it could result in a lot of damages and expensive repairs or replacements. In order to ensure that our data center's environment is optimal for server function, we will need at least to monitor the temperature, humidity, and airflow. Fire monitoring can also be implemented for security reasons.

Before explaining how our control system is supposed to work, it should be a good idea to show how the cooling of a data center looks like. The following Figure 3 will be further explained.

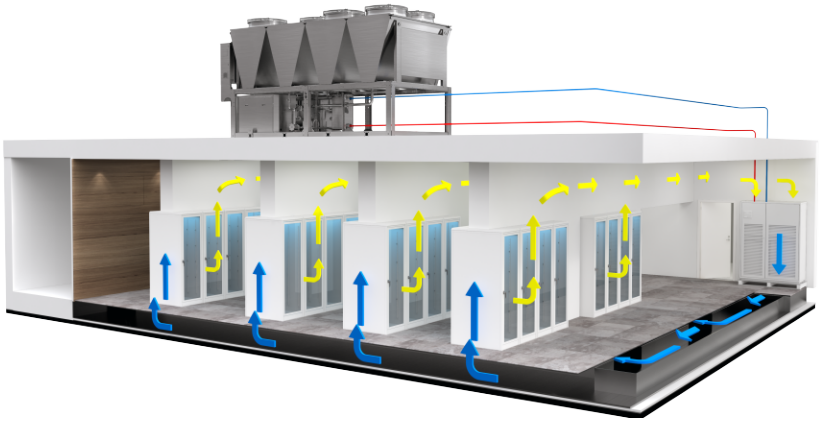


Figure 3: Cooling system of a Data Center

As shown in Figure 3, three chillers on the building roof are responsible for pushing down the air into the building, air that will go down on the floor level, and will cool down the servers by coming out of holes in the ground located strategically between the racks. In the case of the CERN data center, the case is slightly different than the image above: we will be facing 10'000 servers to cool down in total. A quick glance on the CERN website can give us a better idea of the functioning of their cooling system [2]:

> "Air conditioning is a major problem for data centres everywhere in the world at the moment. As processors get faster they also get hotter and at the moment we are getting a greater increase in heat than in performance. Rack machines are even worse as they are densely packed with processors. Some of the racks at the computing center contain only a few machines in them since there's not enough cooling capacity now to fill them with more machines. The room was designed with one supercomputer in a corner in mind, not several thousand processors! *To maximize the cooling efficiency, we use a Hot/Cold aisle configuration: the front of the racks are facing each other on the 'cold' aisle and expel heat out in their backs to the 'hot' aisle. The doors and roofs placed in the cold aisles increase efficiency by only allowing cold air into the machines. The cold air comes out from the grills in the floor inside the 'cold' aisles. The cold air is introduced in the building through the big blue pipes coming from the roof and going down to the floor. 3 chillers on the building roof are responsible for cooling down the air.* This process consumes no energy during the winter months where cold air is directly taken from outside."

The website also gives us indications of the amount of servers located in Hungary:

> "A capacity of around 30 % of the capacity of the CERN Data Centre has been installed at the Wigner Data Centre."

We can therefore assume around 3300 servers are located in Hungary, while 7700 are located in Switzerland. As previously said, all the architecture, hardware choices, SCADA system and other parts of this report will be the same for the Hungarian and Swiss data center. These two data centers will communicate with each other. The only difference between the two locations will be in the quantities involved, therefore changing the final cost. This will be shown in further sections.

3.1 How will our control system work

The cooling system can be partitioned into four levels: a division between field level, control level, supervision level, and management level. The first level contains the actors and sensors, it is the interface between the exterior and the software. The next one is the control level where the PLCs are located. Then comes the supervisory level, where the human touch is

made possible thanks to a Human-Machine Interface (HMI). The process data base is also located on that level. The last level is the enterprise one, where the high level orders are taken, such as a change in cooling regulation for example. It is of first importance that the information flows well through the levels in term of time and quality.

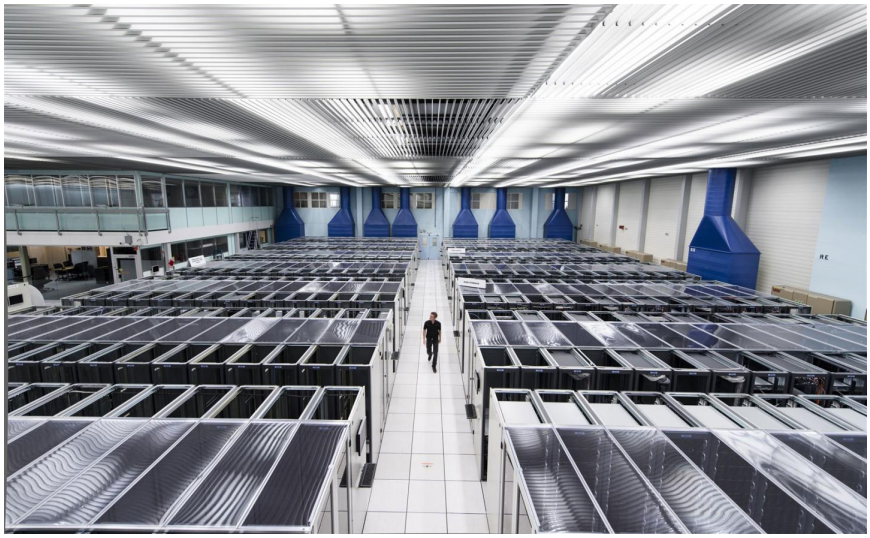
The architecture of the system has been chosen hierarchical and distributed. The reasons are that even if a distributed system is more complex to implement (and more expensive), we are facing a situation where two different countries are involved, with totally different climates and challenges. Distributed System Architecture (DSA) is the ideal solution for integrating processes when there are multiple units, control rooms or geographically distributed locations. With Distributed System Architecture, users experience a single, totally integrated system instead of several independent systems, while retaining the ability to autonomously manage each system. The result: optimum functionality and flexibility.

We chose to implement twice the same hierarchical control system in the two different countries.

Let's see how the system will work in a general way. As we already presented in the previous sections, the aim of our control system is to verify that the temperature and humidity stay within precise ranges. In order to change the values of those parameters, we will use the fans. The velocities of those fans are obviously controllable. Therefore our system will be based on the following components:

- Fans
- PLCs
- Temperature & humidity sensors
- Emergency fire sensors

An other point of this report is to specify the amount of each of those components, and their location on the servers in order to have the highest precision possible to render reality. We based our estimations on pictures taken in the data center itself.



(a) CERN servers

(b) Example of a rack

Figure 4: Swiss CERN data center and a server rack

Based on Figure 4a, we tried to figure out a map of the data center. Counting the racks, we managed to see that the disposal of the servers is the following: 2 row, 7 groups per row, 30 racks per group, so if we consider that there are around 7700 servers in the Swiss Data Center, that makes 18 servers per rack.

As we previously said, racks are positioned in groups that have a cold aisle and a hot aisle, so we only need to put sensors in the hot aisle. The hot aisle is situated between two groups (the cold aisle is inside the group). Hence we can consider putting one temperature & humidity sensor per hot aisle, which totals to 12 sensors for the 14 groups. We can also add four different fire sensors in the cardinal walls of the chamber. The total amount of sensors would therefore be of 16. Figure 5 is a schematic representation illustrating our sensors placement.

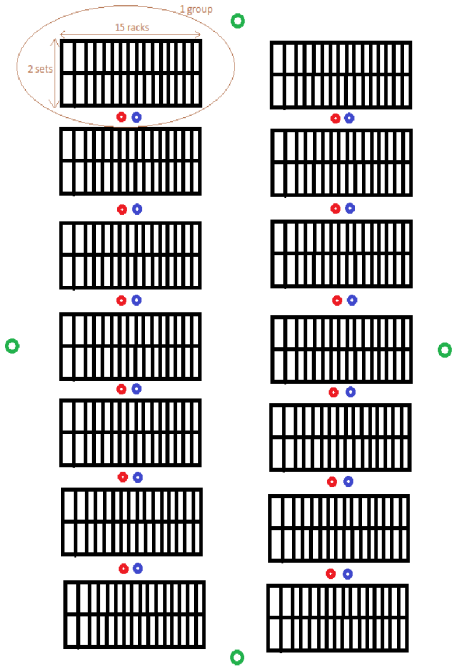


Figure 5: Top schematic representation of the CERN Swiss servers

Red circles represent the temperature sensors, blue circles represent the humidity sensors, and green circles represent the fire alarm sensors. As explained later in Section 3.2 about the hardware, we will use a single sensor for the humidity and temperature measurement (therefore each pair of red and blue circle is a single sensor).

We are now going to broadly present how the different levels (field level, control level, supervision level, and management level) will work, relate and communicate between one another.

On the field level, some sensors will be placed on the servers in order to know exactly both temperature and humidity levels. Those sensors will send analog signal that will be converted into a digital one within the PLC. Ideally, the PLC will be placed close to the fans to allow direct connection to them, sparing connective cables. The speed and accuracy of the information have to be ensured to be efficient in the control of the temperatures and humidity levels, as server's safety will depend on it. Some fire sensors will be placed around the data center. The connections between the PLC and the sensors/actuators are made with Profibus/Profinet field bus which provides robust communications and is compatible with many devices, as we will see in Paragraph 3.3.

We are going to have two PLCs for redundancy in each location. The PLCs are going to measure and evaluate the measurements received against the values for defined by the management team: in our case, the ranges of temperature and humidity levels indicated in Fig2.

If the measured temperatures are lower than the smallest end of the ASHRAE's range (18°C), fans should decelerate. If they are higher than the largest end, fans should accelerate. In order to do so, the PLC will send an order to the actuators in order to modify the velocity. Conversely, we know that the larger the volume of fresh air brought in from the outside, the lower the relative humidity inside. So if humidity levels are lower than advised, fans should decelerate, and if humidity levels are higher fans should accelerate.

We will implement two PLCs per data center. They will work in parallel in order to have redundancy and therefore security over possible failures. The first PLC will operate on the odd numbered temperature and humidity sensors, on two fans and on two fire sensors, while the second PLC will operate on the even numbered temperature and humidity sensors, two fire sensors and one fan. If some fans are not working, or if sensors measure that humidity or temperature stay too long in a certain range, then the PLC should send a warning packet to the SCADA. The SCADA system, through a HMI, will be showing and controlling the two PLCs. In case of an emergency scenario (Emergency Button, critical levels measured by sensors, broken connections between hardware, lost server connections, fire) all the fans are put to full speed level to guarantee a maximum air flux in the data center, as humidity is less of a temporal problem than temperature. When the alarm does not switch off after certain time threshold, a special group of experts within CERN's organization is automatically alerted.

Air circulation should increase and decrease according to the amount of activity from the servers. We make the assumption

that activity is estimated by monitoring the number of servers that are functioning, in order for the fans to have an average value to follow. Then our control system will implement tiny changes depending on the informations received from the sensors.

Here also, PLC's role is of vital importance, as they need to understand when changes should be done to the ventilation. Between the two data centers, communication will be possible thanks to the optic fiber lines. At the Supervision level, we can install a database coupled with a back-up database to be able to extrapolate knowledge from data: one could see how the seasons influence temperature and humidity values, in order to better detect when something goes wrong. The connections between the PLCs and the SCADA system is done via Ethernet.

3.2 Hardware

Sensors

Different kinds of sensors will be used in order to monitor the cooling system. The choice of the sensors has been done by comparing several types. Finally, the multitask sensor Siemens QFA31 was chosen. This device can measure the temperature and relative humidity with great accuracy and in a short period of time. It is meaningfully designed for cooling systems, with auto-correction to possible faults and short times of answer.

In addition, an airflow sensor is also needed to control the velocity of the air flowing throw the pipes. The Siemens QVM62.1 has been chosen for this purpose. The fire sensors will be the Siemens OH720 model. These fire sensors work under harsh conditions like dust.

(a) Siemens QFA31 temperature and humidity Sensor

(b) Siemens QVM62.1 airflow sensor

(c) Siemens 0H720 fire sensor

Figure 6: Siemens QFA31, QVM62.1 and 0H720 sensors

PLC

The PLC is the device used for controlling the whole cooling system, programmed before-hand. The sensors are connected to the PLC, which will analyze the physical signals received from those sensors and will decide whether to actuate or not. The S7-300 (Figure 7a) is suitable due to its ratio quality/cost and because it covers all the operations a cooling system needs. On top of that, it connects to the inputs/outputs by Ethernet or PROFIBUS. The CPU installed will be the model 315-2DP.

(a) Siemens S7-300 PLC [7]

(b) Siemens G120 Electrical Drive

Figure 7: Siemens S7-300 PLC and G120 electrical drive

Electrical Drives

For the electrical drives controlling the motors of the fans, the Siemens SINAMICS G120 (Figure 7b) (4kW, 400V) are used because of their wide applicability and reliability. This compact model is capable of vectorial control and has PROFIBUS connections.

It might be remarkable to add that all the components have been purchased from SIEMENS for various reasons. Firstly, the system should have more integrity if all the devices come from the same brand. Secondly, this company has experience with this kind of installations, they could provide some advice when building up the system. Finally, buying all the material from the same company usually has a better purchasing offer.

3.3 Communication infrastructure and protocols

From a communication point of view, the data center cooling system can be divided in three main parts.

The first part represents the communication between different control/management structures like the management board, archives, etc... This communication level is implemented through the usage of Ethernet (LAN, IP network), as it is a cheap and simple solution, widely available in many PLCs and does not usually require any special device to connect with regular computers, such as the operator workstation.

The two other parts of the communication structure are related to cooling control: in fact, it is the main aspect of this project. On one hand we have communication between SCADA and the PLCs on the control bus, and on the other hand we have the fieldbus that interconnects the PLCs with the sensors and actuators that are physically attached to the servers and fans.

The real time requirements can be divided in two categories. In case you must absolutely hit every deadline, we call it hard real-time system. Otherwise we call it soft real-time. Very few systems have the hard real time requirement: some examples are nuclear systems, some medical applications such as pacemakers... In our case we can miss some deadlines, therefore we do not need hard real-time.

Our sensors will have different behaviors. The temperature and humidity sensors located on the servers will send data at fixed time intervals even if the state is unchanged compared to the previous interval. Due to measurement noise and other effects, it is likely that collected data will change continuously over time anyway. The value from the temperature and humidity sensors should be acquired periodically, but the acquisition frequency does not need to be extremely fast (we expect the temperature and humidity levels to change slowly over time). Here, we can assume information is sent every 30 seconds. This will allow us to have a drastic control over the servers state, so that in case of a major change in something (the fans stop working for example), the event can immediately be detected just by analyzing the temperature and humidity changes. In addition to those sensors, we also have some fire sensors that will work differently, in a discrete way and only activated on an event basis.

Although 4-20 mA has been the main field signaling standard, modern DCS systems can also support fieldbus digital protocols, such as Foundation Fieldbus, profibus, HART... Fieldbus is the name of a family of industrial computer network protocols used for real-time distributed control, standardized as IEC 61158. A complex system to be controlled usually needs an organized hierarchy of controller systems to function. In this hierarchy, there is usually a Human-Machine Interface (HMI) at the top, where an operator can monitor or operate the system. This is typically linked to a middle layer of programmable logic controllers (PLC) via a non-time-critical communications system (e.g. Ethernet). At the bottom of the control chain is the fieldbus that links the PLCs to the components that actually do the work, such as sensors, actuators, electric motors.... We are now going to talk precisely about the fieldbus.

Choosing a bus at the field level instead of connecting each sensor individually to the controller using protocols such as 4-20mA can be easily justified. First of all, fieldbuses require only one communication point at the controller level and allows a multitude of devices to be connected at the same time reducing both the length and the number of cables required. Most importantly, buses are designed for robust transmission over long distances, implying that the quality of the signal is less likely to decrease. We now have to chose specifically which fieldbus to use. After comparing different types, we chose to implement PROFIBUS [4] for the reasons listed below:

- It is supported by many vendors of field devices (sensors, actuators...) which involves a big product choice on the market
- There is a constantly renovated technology development guaranteeing the continuous development of the technology.
- PROFIBUS can tolerate up to 32 devices, allowing easy incorporation of multiple devices.
- It is supported by PI, the world's largest fieldbus organization.
- It can support the real-time demands at this level for time-critical events that can happen during the operation of the system and need to be monitored and controlled quickly.
- Completely suitable for the dimensions of the system [1]

Two PROFIBUS communication protocols are used at the field level as seen earlier. Two kinds exist: PROFIBUS PA is supported by the sensors, whereas PROFIBUS DP is supported by the actuators (fans).

The PROFIBUS PA protocol can support both event-driven and cyclic transmission of data which is perfect in our case, as we have both temperature and humidity sensors that are cyclical, while the fire sensors are event-driven.

When it comes to the communication between SCADA and PLCs the MMS protocol seems to be a good choice. MMS (Manufacturing Message Specification) is a messaging system for modeling real devices and functions, for exchanging information about the real device, process data - under real-time conditions - and supervisory control information between networked devices and/or computer applications. It can deal with mixed data traffic (both cyclic and event-driven) as well as work in Read and Write modes. From a security point of view, it contains an authentication mechanism.

3.4 Bandwidth estimation

In order to achieve efficient communication within the same level and between different levels, an adequate bandwidth is necessary. However, the estimation of the bandwidth usually is quite difficult, not precise and variable but not in our case. The low sampling frequency of the sensors make the necessary bandwidth very small.

Assuming that the sensor measurements are updated every 30 seconds and that the size of a standard PROFIBUS message is around 250 bytes, the required minimum bandwidth for the whole data center is around $(250 * 16)/30 = 133$ Bytes/s, which can be easily satisfied by PROFIBUS, even if we decide to add other sensors to the system.

4 P&ID

The P&ID of the system is shown in Figure 8. Although the diagram tries to be as precise as possible, not all the temperature and humidity sensors are represented, since there are quite a few of them.

The stripped lines represent electrical signals, while the continuous lines represent physical transmissions, such as the connection from the motor to the fan. Nevertheless, the two lines representing the pipe are just to make it easier to analyze the P&ID. In addition, a legend is available with the meaning of the letters and symbols, including the total number of devices used in the system.

There are two main circuits in the system. The first one, defined by red lines in the P&ID contains the odd numbered temperature and humidity sensors (only the first and the last one are included) as well as the first and fourth fire alarms. It goes to PLC 1 and it takes control over fan 1 and fan 2. The second circuit, represented by black lines is determined by the even numbered sensors of temperature and the third fan. The fire alarm is controlled by both circuits.

Although not represented in the system, two airflow sensors go to the circuit 1 (black) and the third sensor is part of circuit 2 (red). It is also remarkable that the notation in Tango start from 0, and here from 1.

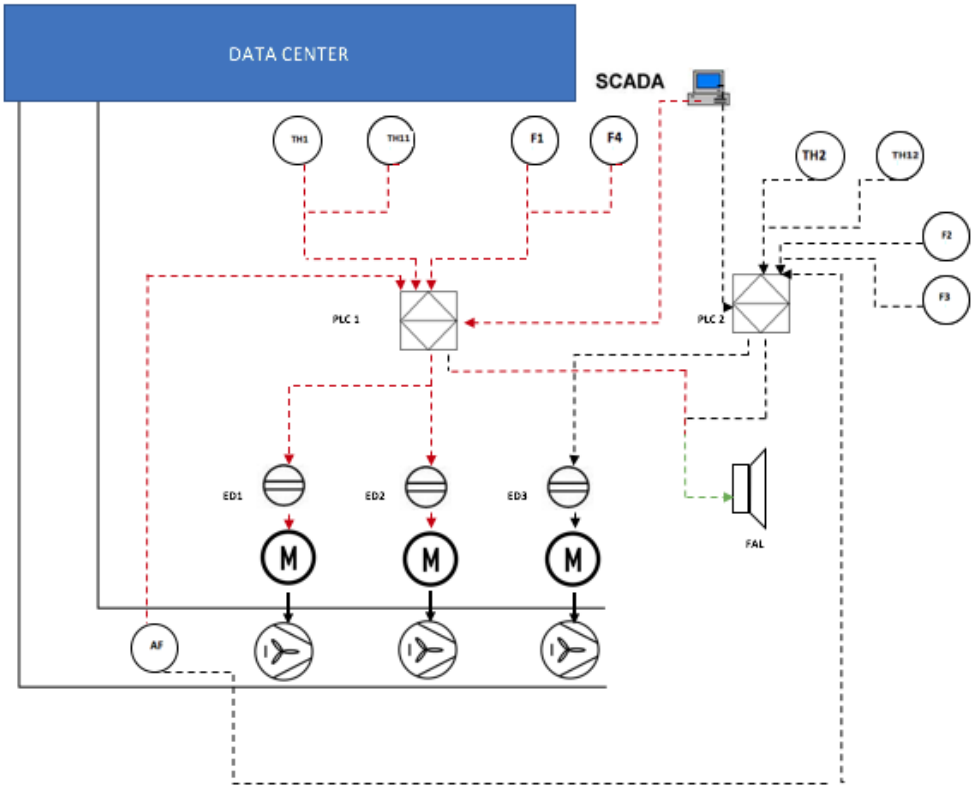


Figure 8: P&ID representation of the system

SYMBOL	LETTER	MEANING	NUMBER	MODEL
F1	F	FIRE SENSORS	4	0H720
AF	AF	AIR FLOW SENSOR	3	QVM62.1
TH1	TH	TEMPERATURE AND HUMIDITY SENSOR	12	QFA31
	ED	ELECTRICAL DRIVE	3	G120
M	M	MOTOR	3	GIVEN
	F	FAN	3	GIVEN
	FAL	FIRE ALARM	1	GIVEN
	PLC	PROGRAMMABLE LOGIC CONTROLLER	2	G7-300

Figure 9: P&ID legend with all the elements that compose the system

5 Description of SCADA implementation

Our SCADA system is implemented using the Tango software [3]. It allows monitoring of both CERN's data center locations, but only allows the data center in which it is installed to be controlled. The system presented here would be installed in the Swiss data center, therefore it can monitor and control it, while only monitoring the Hungarian data center.

5.1 Device servers

The SCADA system in composed of 3 distinct device servers: "IA_VentilationDeviceServer_01" (epfl/vds/1) and "IA_VentilationDeviceServer_02" (epfl/vds/2) are used to simulate PLC1 and PLC2 of the Swiss data center, whereas the device server "IA_HungarianDatacenter" (epfl/vds/3) abstracts the Hungarian extension.

Moreover, the "data center_simulator" script is used for debugging and for simulation purposes. It changes the value of various sensors to trigger some alarms and it makes the temperature change depending on the "load" of the servers, in order to showcase how our monitoring and controlling system performs. It also logs in a file all the sensors/actuators values, as well as the alarms' states.

The fans have their speed adjusted depending on the different alarms states and priorities. The priorities, from highest to smallest, are: fire alarm, temperature alarm, humidity alarm. In case of fire the fans turn off so they do not feed it in oxygen, in case of high/low temperature they gradually increase/decrease in speed, and finally, in case of high/low humidity they gradually increase/decrease as well.

In our system, each data center houses 12 temperature sensors, 12 humidity sensors, 4 fire sensors, 3 air flow sensors, 1 external humidity sensors, 3 fan actuators and 1 fire alarm.

All those sensors and actuators are evenly distributed between the two device servers for the Swiss location such as specified in the P&ID, but for the Hungarian location they all are handled by the single device server. Two commands to set to 0% or 100% all three fans of the local data center are also available. The specifications of each attribute representing a sensor/actuator are present in Table 1.

Attribute	Type	Permission	Function
temp_00..11	DevFloat	Read-Only	Sensor
hum_00..11	DevFloat	Read-Only	Sensor
air_flow_00..02	DevFloat	Read-Only	Sensor
fire_00..03	DevShort	Read-Only	Sensor
fan_00..02	DevFloat	Read/Write	Actuator
fire_alarm	DevShort	Read-Only	Alarm
hum_alarm	DevShort	Read-Only	Alarm
temp_alarm	DevShort	Read-Only	Alarm
air_flow_alarm	DevShort	Read-Only	Alarm

Table 1: Specifications of the attributes

5.2 Human-Machine Interface

The HMI is composed of two panels (Figure 10a & 10b): one for each data center location. Both have a main area where the overall status is displayed, and where a "Sensors details" button allows a detail area with every sensors values to be visible or not.
The panel for the Swiss data center also includes a "Ventilation system" section so that the operator can interact with the fans by either starting/stopping them all, or by setting a particular value to each.

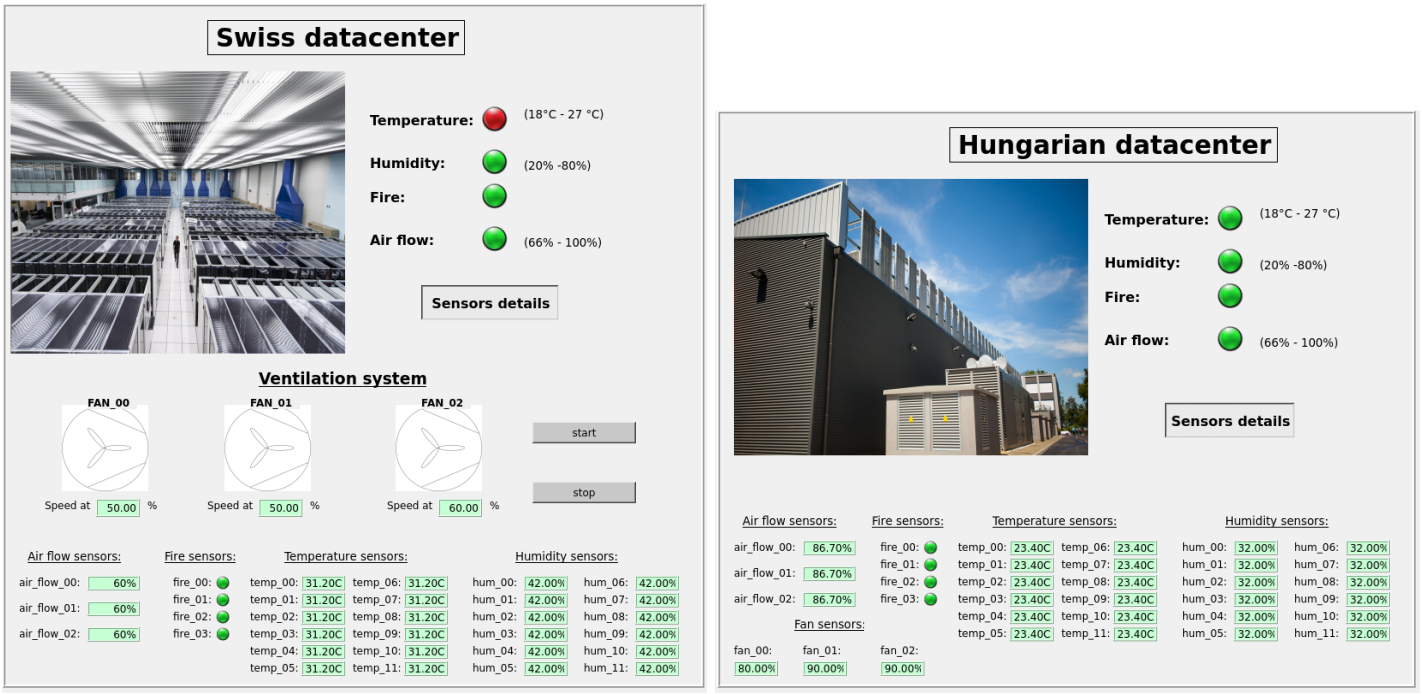
6 Security analysis

6.1 Failure mode and effect analysis (FMEA) and reliability

The FMEA is given in annex in a excel document (of course this document is only a first approach of the FMEA and only contains the main failures, thus it is not as exhaustive as a real FMEA should be).

Some general comments about the reliability of our cooling system :

- The reliability of our system is mainly ensured thanks to redundancy of the vital parts of the cooling system.
- The redundancy of the temperature and humidity sensors is ensured as we have 12 of them in each center.
- The same goes for the airflow sensors (as we have 3 of them).
- As we have 3 fans per center, if a failure occurs in 1 or 2 of them (or in their electrical drives), we can still ensure the cooling of the servers while we are putting them in a safe state of and/or repairing them.
- We divided the sensors into 2 groups linked with 2 different PLCs (through 2 different PROFIBUS) to create a redundancy and not to have a system depending solely on a single correctly functioning PLC and fieldbus.
- Periodic check-up of all the physical devices should be performed.



(a) Swiss datacenter panel

(b) Hungarian datacenter panel

Figure 10: HMI for our SCADA system

6.2 Cyber-security

As our system is implemented in a data center, it makes it particularly sensitive to cyber-attacks. Indeed, the attacks could be done in numerous different ways and for many different reasons, such as:

- A Trojan could attack the cooling system to take control of it and making it operate incorrectly.
- Attacking the cooling system could be seen as a way for the hackers to reach the data stored on the servers (that's why we must separate completly the softwares of the cooling system and the data management system, then there are no problems).
- Attacking the cooling system could be a way to reach any other software of the CERN (same remark as the previous one : separation of the software, the software of the cooling system must be completely isolated)
- The attack could come from a malware that hid on the servers or on any other software of the CERN (if the softwares are not totaly separated).

So ensuring the cyber-security of this cooling system is not only necessary to ensure a correct functioning but also to protect the data stored in the servers and by extension the whole CERN network.

The first advice is to implement segmentation. This means that we have to subside the system in as many logical sub networks as possible. For example, in our cooling system, we have two systems (echo with one half of the sensors and PLCS) which should be separated in two subsystems not interacting together (they only interact with the higher levels).

To have an efficient defense system, we must implement a "defense in depth", meaning that we must ensure the security at every level of our plant. This creates a redundancy of controls and safety protocols.

- At the physical level, we must prevent any unwanted access to our systems by controlling and restricting the access of the different physical parts of the centers. We should ensure that someone should be able to have access only to the areas he actually needs. For example, only the administrators responsible of the control should access the control room.

  The fact that we have two centers related by fiber optic lines across several countries can make our system particularly sensitive to attacks during data transfers. Indeed, it is nearly impossible to control who would access those lines, thus the data must be protected during the transfer. That means encrypting it.

- At the network level, we must ensure that we have firewalls at each interconnection between each segments of our network. Furthermore, we should make sure that each part of the software has access to and can modify only what it needs. For example, the SACDA system has Read-Only access to temperature, humidity and fire sensors to make sure it cannot tamper them.

- At the computer level, we must ensure that they are well protected (anti-virus, firewalls,...) and that there is no interference with other networks. That is why we highly recommend to ban any external removable computers and USB keys from the system.
- At the access level, we can recommend to implement some authentication systems and to ensure the safety (personal passwords changed regularly, restricted accesses,...).

In addition, scans of all the software should be done regularly to try to detect any malware hidden in the system. Indeed, a malware can hide for years waiting for any opportunity to attack. Therefore, it is necessary to have regularly security reviews and audits to evaluate the cyber-security of the plant. Moreover, do not forget to update regularly the system and to remove any unneeded application. Indeed, the life expectancy of our cooling system is much longer than the amount of time we can expect any cyber-security system to ensure a good safety.

To conclude this cyber-security analysis, we must make some general warnings. The cyber-security cannot be ensured as it is a race between hackers and security experts to find vulnerabilities and countermeasures. So our objective to protect our system is to make sure that it is protected for any known threat and to try to find any breach that might be used. The zero risk does not exist for computer system but regular check-ups and updates can reduce that risk.

6.3 Recommendations about cyber-security

Now, we are going to hive you concrete recommendations that result from the previous cyber-security analysis. So to ensure an efficient security of th computer system we should :

- Segmentation of the network
- Restricted accesses to the plant and software
- Use of strong firewalls
- Ban any removable devices (laptop and USB keys)
- Encryption of data during transfers (especially between the two part of the plant)
- Efficient authentication system (personal and regularly changed passwords)
- Regular scans and updates of the software

7 Cost estimation

The costs were estimated by choosing an average price for the devices used in the project (this is the cost for one of the Swiss plant).

Device	**Model**	**Quantity**	**Price/unit ($)**
Electrical drive	G7-120	3	602
Airflow sensor	QVM62.1	1	184
Fire sensor	0H720	4	80
Temp. & hum. sensor	QFA31	12	384
PLC	S7-300	2	1260
		Total	9438

Table 2: Cost estimation

The cost of the hardware would rise up to 9438$ per data center, so 18876$ in total.

Also, we need to point out that the software and installation costs are not taken into account, as the data was not sufficient to have a precise forecast. These far exceeds the hardware costs since they require human labor.

8 Conclusion

Our purpose in this report was to present a solution for implementing the automation of the cooling system of the CERN's servers. We presented a system architecture for this cooling system and we chose the hardware (sensors, buses, PLCs, ...) needed for the system. Then, we presented a solution for the SCADA software. Finally we added a safety and security evaluation of our proposed solution.

This report is only the first step to implement the cooling system. Indeed, a longer and more in-depth study should follow this report. Our goal was only to provide a first solution and some recommendations of what is needed to implement an efficient, safe and reliable cooling system in the CERN's data centers.

References

[1] *https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6XV1830-0JH10*

[2] *http://information-technology.web.cern.ch/about/computer-centre*

[3] *http://www.tango-controls.org/resources/documentation/*

[4] *http://www.profibus.com/technology/profibus/*

[5] *EPFL Inductrial Automation lessons by Dr. Yvonne-Anne Pignolet and Dr. Jean-Charles Tournier*

[6] *https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=20093*

[7] *https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=20115*

[8] *https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/C79000-G7300-C185*

[9] *http://w3.siemens.com/mcms/mc-drives/en/low-voltage-inverter/sinamics-g120/pages/sinamics-g120-portlet.aspx*