HIGH AVAIBILITY FOR COMPUTERS RUNNING HMI SOFTWARE – ZERO DOWNTIME

J.D. GODOI[1], R. R. MALDONADO[2] e J. D. TAGLIAFERRO[1]

[1]Faculdade Municipal Professor Franco Montoro, Engenharia Quimica.
[2]Universidade Estadual de Campinas, Departamento de Alimentos.
Contact e-mail: ratafta@yahoo.com.br

ABSTRACT - The HMI (Human Machine Interface) software running on computer COTS (Commercial Off The Shelf) has brought to the industry a higher cost-effective ratio and has become a widespread technology in industrial process control. Ensuring that this system is always available is a large industrial concern, since these computers oversee continuous reactors, evaporators, spray dryers, etc. The control room becomes the pulsating center of the plant and ensures the loss of only a few minutes of operation. With the advent of virtualization, this system has become reliable and feasible for industrial process control environment. This article aims to show a project that integrates PLC (Programmable Logic Controllers) to servers (Process Control) with HMI/OPC remotely connected to virtualized thin clients located in control rooms. This virtualized environment generates a solution with near zero downtime and ensures that in the event of disasters, the recovery of the entire system environment can be done in minutes.

1. INTRODUCTION

Nowadays industrial equipment are virtually all automated, so operators need computers with software and networks dedicated to the control and monitoring of the process. In this environment, all channels should have control rooms strategically located close to the production, in which operators can monitor and control all equipment through that computer system (Mogensen, 2013).

Virtualization started with the use of autonomous computers dedicated to the production channels. Each computer worked independently of the other production systems. However, with the development of technology in production and control there was a need for integration between the channels of production, and consequently it became necessary to interconnect the control computers, giving rise to a central control and monitoring (Lindfors, Kivelä, 2012).

These data centers have servers that collect input from PLCs and deliver this information to the operation, in the form of graphs, in the control rooms. In addition, they receive commands from operators via keyboard, mouse and more recently, touch screen to be taken to productive channels.

Ensuring that the service is always available is a priority of the process. The continuous operation of reactors, dryers, evaporators, storage products, consumption in tanks and numerous other processes are totally dependent on the virtual control. Loss of control, even if temporary, could mean many lost hours or products out of specification The interruption of reading of pH, temperature, pressure and other parameters can lead

to loss of many hours of operation until the production parameters are recovered. Additionally, any product produced during the turbulence needs to be reprocessed or discarded (Flint, Neland, 2011).

The aim was to ensure that the virtualized service never stops or, in extreme cases, that the re-establishment of the system occurs as fast as possible. Computer equipment and software were developed to improve the reliability of the whole system of monitoring and control. The virtualization solution for computers is already being applied in the IT industry for some time in a very reliable and feasible way.

2. AUTOMATIC PROCESS CONTROL

Supervisory control and data acquisition (SCADA), distributed control system (DCS) and programmable logic controllers (PLC) are the basic systems to allow an automatic process control (Payne, 2010).

The PLC, along with a client-server software human machine interface (HMI) is a solution for centralized monitoring and control through networks of long-distance communication. The information is received by the remote PLC distributed along the production channel. The servers handle and deliver information via work station customers in the halls of controls. These data give support to the operators so they can take some action. Field devices control local operations such as opening and closing valves; sensors collect data and monitor the local environment for alarm conditions (Stouffer, Falco and Kent, 2006).

3. VIRTUALIZATION

Virtualization is a technique that allows a computer system to be divided into multiple isolated execution environments, similar to a single physical computer. These environments are called virtual machines (VM). Each VM can be configured in an independent way and have their own operating system, applications, Internet services and network parameters. It is possible to interconnect virtual machines as if they were physical machines. Some virtualization tools support virtual network such as switches and routers. Firewalls and VPN can also be used between VMs (Carissimi, 2008).

While virtualization has been a part of the IT landscape for decades, it was only in 1998 that VMware gave the benefits of virtualization for x86 industry standard platforms, which now form the majority of PCs, notebooks and servers. A key benefit of virtualization is the ability to run multiple operating systems on a single physical system and share hardware resources.

Nowadays virtualization can be applied to a range of system layers, including hardware-level virtualization, virtualization in an operating system level and virtual machines in high level language. Hardware-level virtualization on IBM mainframes pioneered in the 1970s, and then, more recently, suppliers of Unix/RISC began with partitioning resources based on hardware before moving to software-based partitioning (VMware, 2006).

The Figure 1 shows the virtual infrastructure.

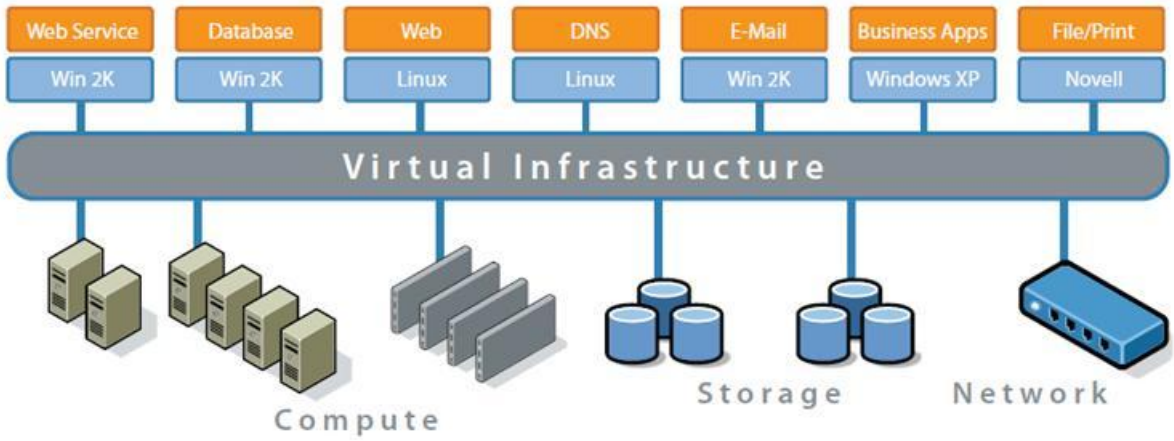

Figure 1: Hardware/Software Separation.

4. WORK ENVIROMENT

This article studied the environment of chemical/industrial food production with continuous process without interruption periods and well known equipment for chemical engineering. The environment was designed to work with standalone automatic process control with independent production channels. However, after some years this solution failed to meet production demand. The solution to monitor the development of the production was virtualization. All control and monitoring migrated to virtualized environment of computers and supervisory HMI software system (VMware, Dell, Rockwell Automation, 2014).

To this solution were required four servers in rack with processing and memory four times higher than the necessary to the system, two storages and four iSCSI switches, provisioning a network of remote storage with access to all hosts. The equipment was installed in two separate buildings at a distance of approximately 600 m. The communication link between them was made with dual route through optical fiber. In the control room the old PCs were used for remote connection to the new server via Microsoft's RDP service and new operator stations were installed by Thin Clients (for Wyse T50).

The software used were:

- Control and Process Monitoring: Factory Talk View SE (HMI), RSLinx Enterprise (OPC), Windows Server 2008 R2 (OS), Windows Server 2012 (AD), Symantec Endpoint Protection (Antivirus), Microsoft SQL 2008 R2 (Stock data).
- Virtualization, VMware vSphere: ESXi (Hypervisor), vCenter (Management), vSphere Data Protection (Backup).

The servers were installed in 4x4x2 configuration, being physically installed 2 hosts, 2 switches and 1 storage in each building. However, virtually only one cluster was created, which causes the system to operate in a unique environment. This strategy provides more features and enhances availability in case of physical faults. The equipment was designed to support the entire system without loss of service, using only one server, so the system understands that the environment is only one providing more resources and increasing availability in the event of physical failure. These devices were sized to support the entire system without loss of service, with only 1 server, 1 switch

and 1 iSCSI storage. Thus the system supports up to 3 failures (3 hosts, 3 switches and 1 storage) operating without stop and without affecting production. The failure against disaster in the datacenter (such as fire) is covered by the existence of two rooms in separate buildings.

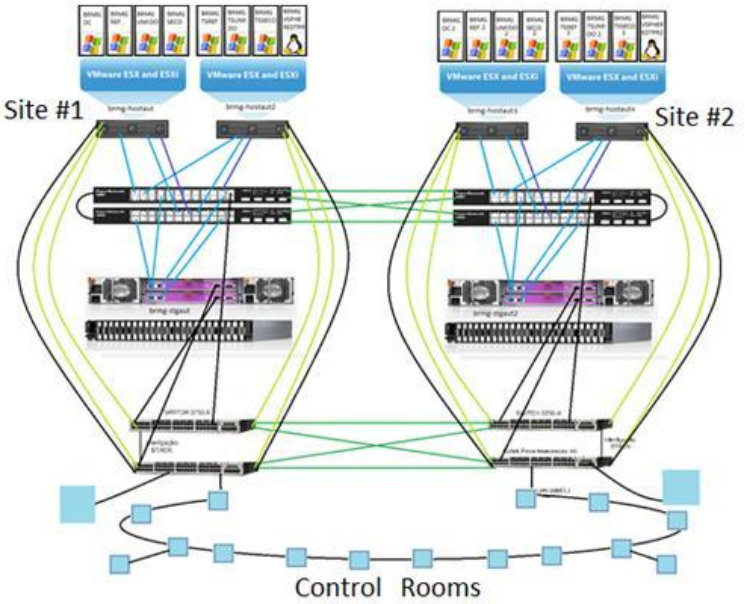

Figure 2: Hardware Architecture

The logic part of the system (software) has two servers for each service, each building. They are: AD for user authentication; FTView SE (HMI) and RSLinx Enterprise (OPC) with redundancy enabled; two FTView Client with RDP which are thin clients, and PC of control rooms connected remotely. PCs and Thin Clients of control and monitoring rooms that get together to productive channels have two screens. Each screen features a different RDP session in FTView Client, where operators can monitor and control the process equipment in the field.

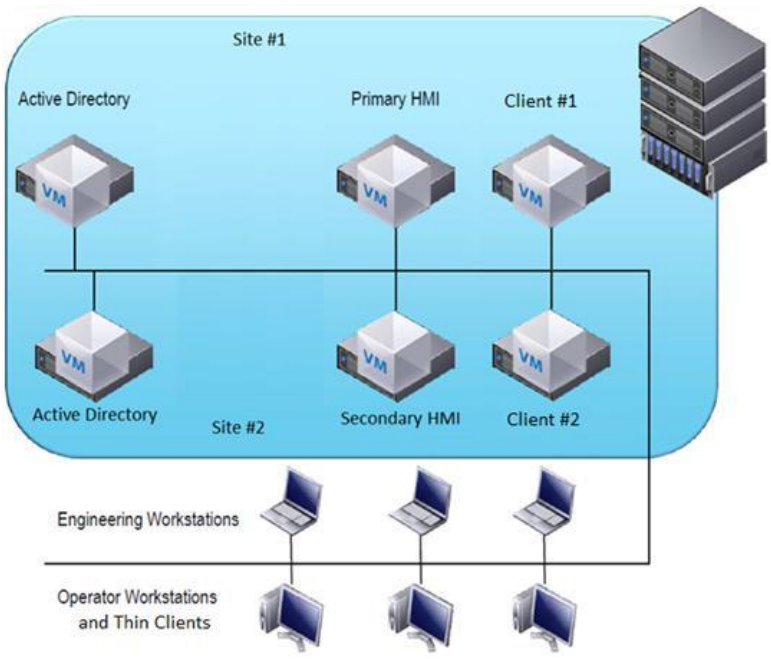

Figure 3: Software Architecture

Hardware redundancy is managed and controlled by the vSphere Suite. In case of failure in the software, each service has a redundant server that automatically takes over if a fail happen in their respective pair.

The complete environment is shown in Figure 4, divided into three layers: layer 2 was the main goal of this solution, composed by the supervisory and servers. The layers 1 and 0 are responsible for monitoring infrastructure and automatic process control.

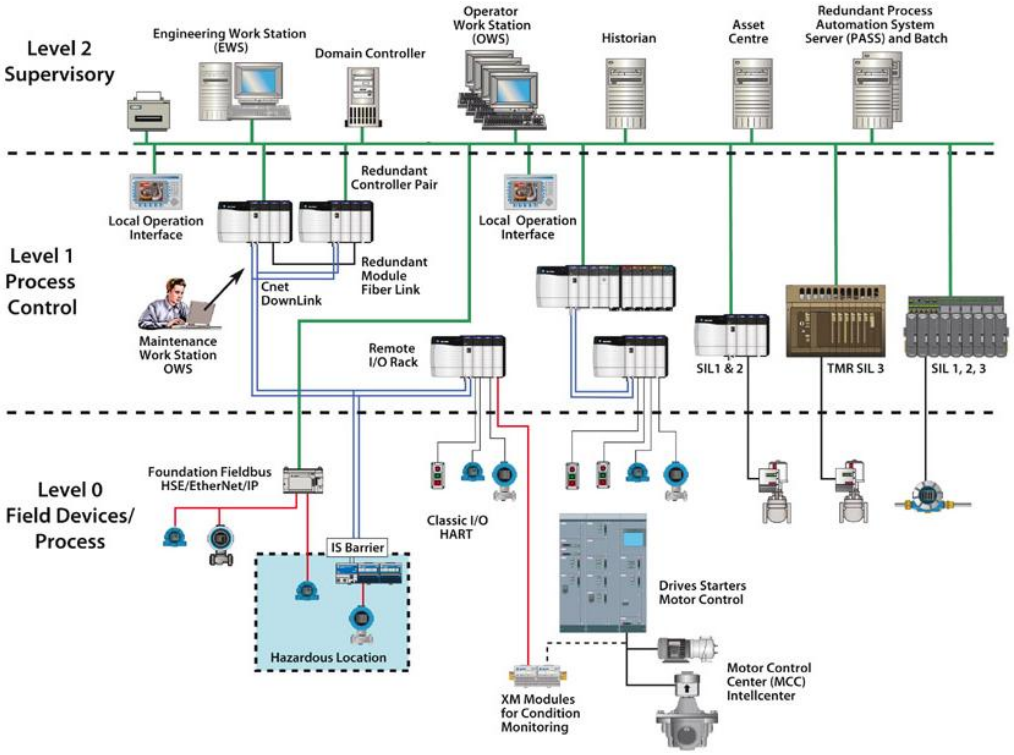

Figure 4: Overall Architecture

5. CONCLUSION

The system now has tolerance to numerous failures, both hardware and software, including disasters, such as fire, in one of the sites. Prior to this work, in the event of failure on a host a period of 24 to 36h to retrieve a new server was necessary if the hardware was available in stock. Complete installation of new operating systems, drivers and dedicated service software, in addition to activation of each software separately, was necessary before. To recover from a disaster of 36 a72h they needed to rebuild an entire site depending on the affected server. Therefore stopping a productive channel or even the whole plant was inevitable.

Now the environment has a recovery time of only 60s in the event of a host failure, which is the time it takes to restart the virtual machine to another host. Failure in HD storage is imperceptible, with tolerance of 3 HD failures per storage. A failure in storage is covered by redundancy via software, since the service servers work in duplicates. The recovery of a complete storage can be done through the backup on all full virtual machines. This assures the possibility to recover a virtual machine in just 30

minutes. In this system, the recovered machine remains the same that worked before failure, no need to reinstall the OS, software, and keeping intact the activations. In the event of a site disaster it can be recovered from the backups, in between 8 and 12 hours, if the hardware is in stock.

However, in none of these cases the process is affected, except for a few minutes in more severe cases, which avoids the stop of productive channels. The physical servers were reduced from 8 to 4, reducing the amount of equipment for maintenance, heat generation and power consumption.

Any maintenance work required of the system, can be done during normal working hours without system interruption, since it is simple to move a virtual machine from one host or one storage to another without stopping its service. Thus one can perform the physical maintenance of a unit or logical virtual machines and return the original unit after maintenance.

It is an ideal solution for production environments that require high availability, leaving the system of monitoring process and control very reliable. The solution provides the flexibility of the actions of maintenance of the OS which is fault-tolerant and with rapid disaster recovery.

6. REFERENCES

CARISSIMI, A. V*irtualização: da teoria a soluções*. In: 26º SIMPÓSIO BRASILERIO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUIDOS, Porto Alegre. Porto Alegre: UFRGS, 2008 p.174-176.

BAILEY, D., WRIGHT, E. *Pratical SCADA for Industry*.Burlington: Printed by Elsevier. 2003.

LINDFORS, N.; KIVELÄ, J. Enhanced Maintanence Efficiency With Third-genaration Control Valve Diagnostics. *InTech*, 2012.

MOGENSEN, K. Æ. Automation Automation Automation. *Scen. Mag.*, 2013.

NELAND, J.; FLINT, F. Beyond controllers and capacitors. *InTech*, 2011.

PAYNE, J. Modern PLCs and PACs pack more punch. *InTech*, 2010.

STOUFFER, K.; FALCO, J.; KENT K. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*. Intelligent Systems Division Manufacturing Engineering Laboratory National Institute of Standards and Technology Gaithersburg. 2006.

VMware. *Virtualization Overview*. White Paper. Palo Alto: 2006.