Fire & Gas Networking and Cyber Security Requirements

Gianbattista Zago
Safco Engineering - Chief Operative Officer

Giornata Studio AIS ISA 28 Marzo Milano

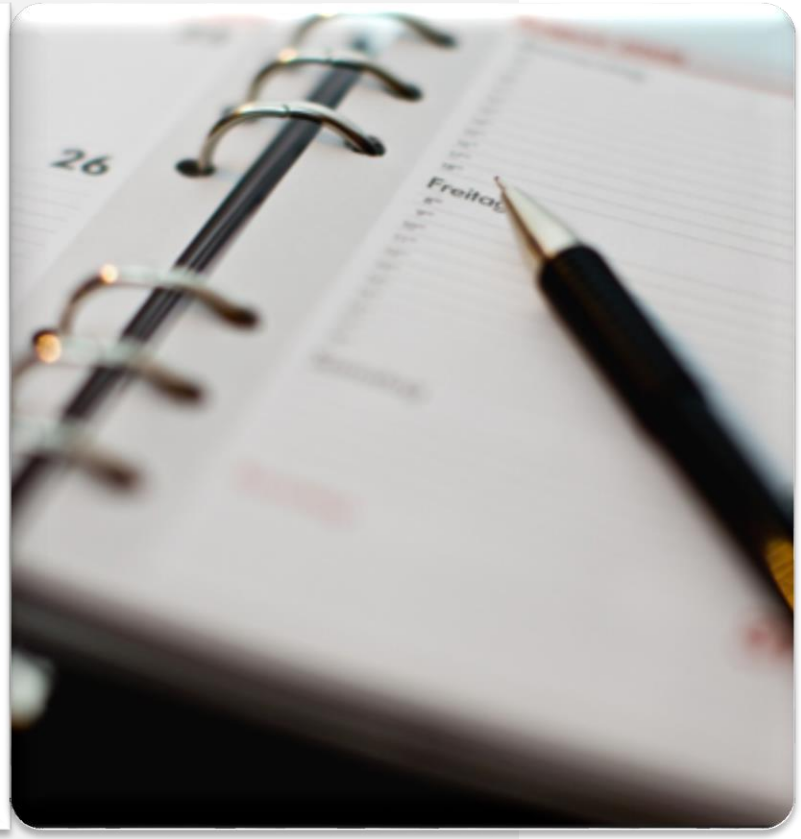
Engineering

"We serve our customers with innovative, compliant, high quality Safety Systems"

AGENDA

REAL CASE

- Fire & Gas Networking
- Virtualization Technology
- Cyber Security Requirements



CASE STUDY: PROJECT REQUIREMENTS

Fire & Gas Networking

The project starting point: the basic design and key requirements

In 2009 SafCo Engineering awarded a large Fire & Gas Detection System Project for one of the biggest refineries in the Middle East.
The basic design provide 94 individual systems interconnected in to a global refinery Fire & Gas network.

- Redundant hot backup controller
- Communication between the systems via redundant fiber optic network ring
- Hot swap of the single components
- Conventional DI & DO for process area devices
- Addressable smoke/heat fire detection system
- Local graphics anunciator LCD based
- Interface with DCS via redundant OPC DA
- Interface with plant alarm managements system with OPC AE
- Time sinchronization between F&G and DCS SNTP protocol

SAFCO PROJECT SOLUTION

Fire & Gas Networking

Evaluating the customer need SafCo Engineering offered an innovative solution

PROJECT PHILOSOPHY

- Multi contractor symultaneous management
- Individual power on of the system without central control
- Individual sub network operation plant are based for DCS interface

SafCo Enginners divide the system into **logical levels** and create a **sub network** to be joined together as part of a **global network**

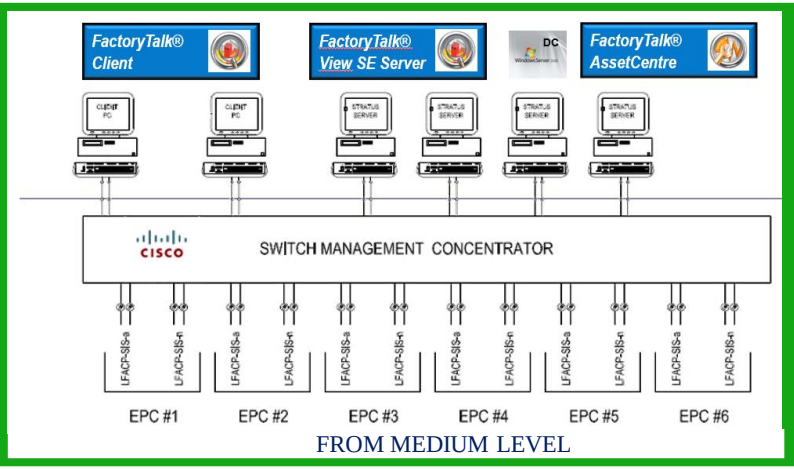
SAFCO provided an **integrated solution** in compliance with the client requisitions developing an **innovative system** which is fully based upon PLANT PAX Process Automation System and SAFCO intelligent fire panel.

THE SYSTEM ARCHITECTURE LEVELS

High Level (HL)

High Level (Lower + Medium) = HL

Main servers dedicated for data collection, disaster recovery and domain control of the network



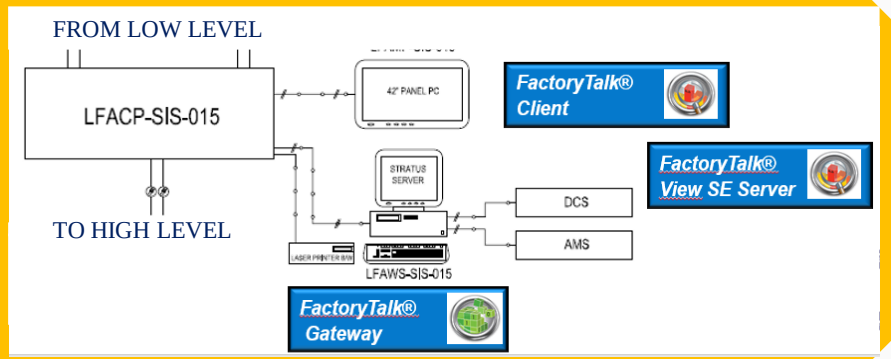
Medium Level (ML)

Medium Level = ML

Local F&G panel for building and process area protection

Local server for data collection and interface with DCS and High level

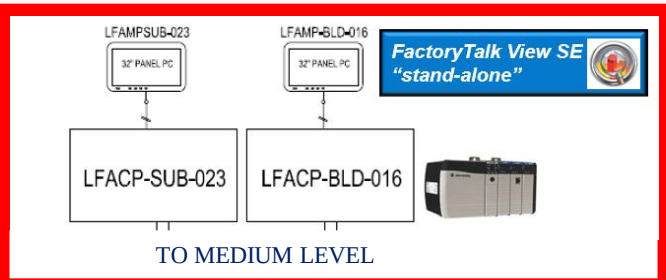
Medium and lower level graphic interface HMI (client of local area server)



Low Level (LL)

Lower Level = LL

Local F&G panel for building protection with stand alone graphic interface HMI



THE REDUNDANCY

Fire & Gas Networking

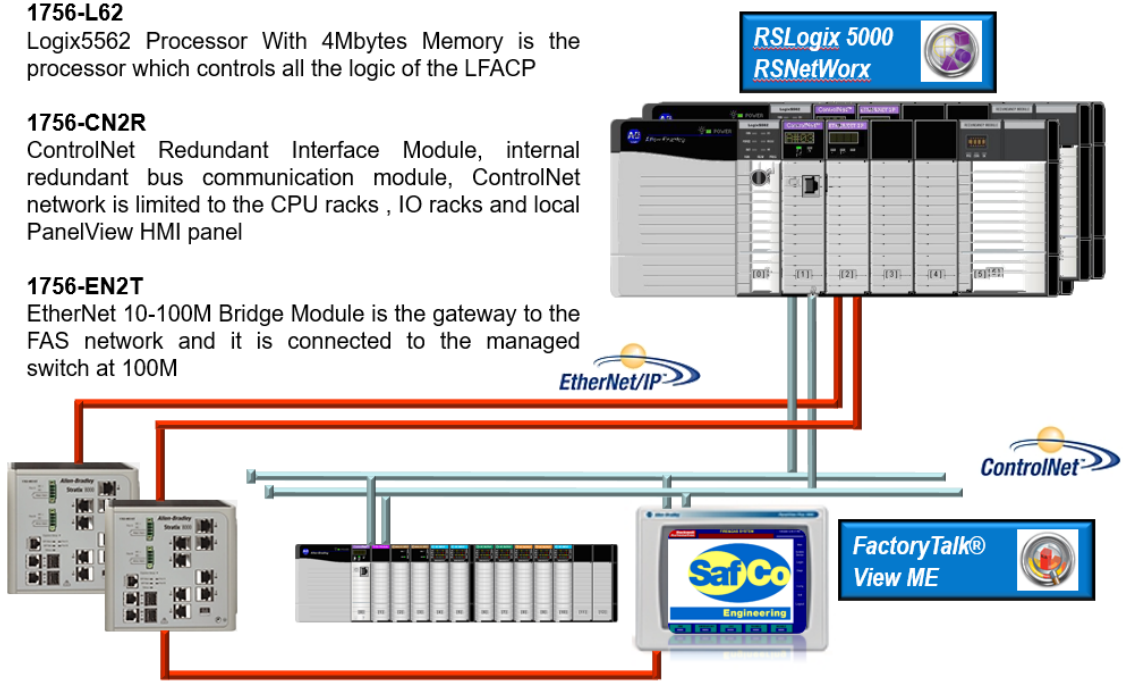
An efficient and reliable Redundancy for both System both Network was installed

SYSTEM REDUNDANCY

1756-L62
Logix5562 Processor With 4Mbytes Memory is the processor which controls all the logic of the LFACP

1756-CN2R
ControlNet Redundant Interface Module, internal redundant bus communication module, ControlNet network is limited to the CPU racks , IO racks and local PanelView HMI panel

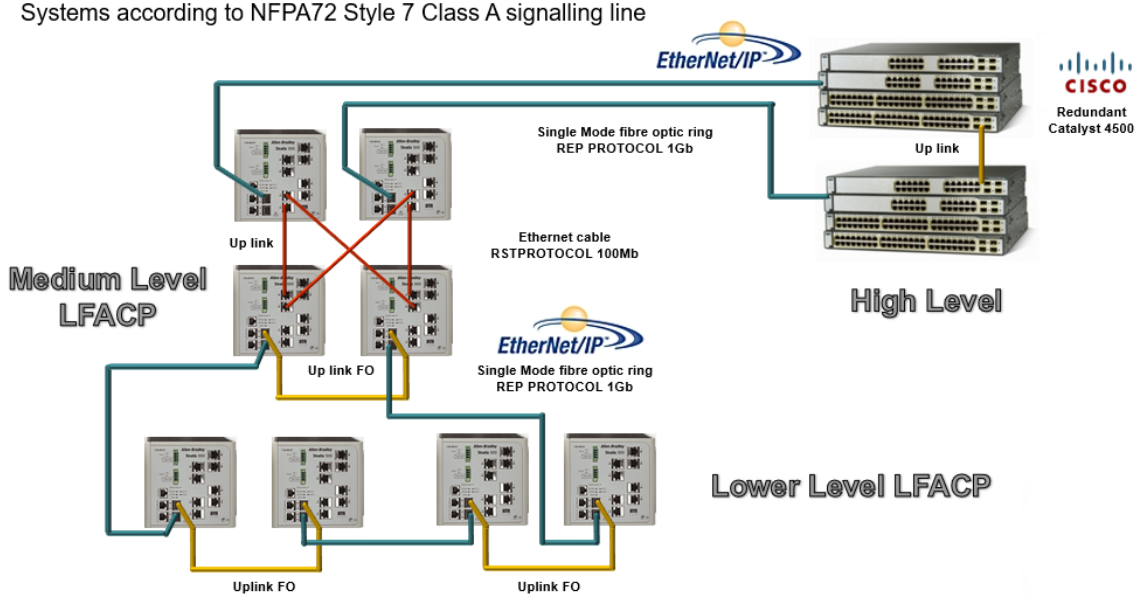
1756-EN2T
EtherNet 10-100M Bridge Module is the gateway to the FAS network and it is connected to the managed switch at 100M



NETWORK REDUNDANCY

Redundant intelligent Allen Bradley Stratix 8000 managed switch is installed inside the LFACP for Ethernet fibre optic media conversion

100Mb Up Ring link shall be provided between the two redundant Stratix 8000 switchs in order to realize a closed ring communication channel between Low Level and Medium Level Systems and High Level Systems according to NFPA72 Style 7 Class A signalling line



THE DETECTION SYSTEM & ALARM DEVICES

Fire & Gas Networking

*A complete and complex **Conventional F&G detection system** and relatives alarm devices were implemented*

F&G detection system is controlled by 1756 cards, all signals incoming and outgoing from the IO cards are line monitored according to the project specification and safety requirements.

All signals are processed by the controller and relevant alarms are displayed on the local HMI and in the main operator HMI.

RSLogix 5000
RSNetWorx

Building
Gas detectors
AI

Process
Flame Detectors
AI

Process
Pressure Transmitter
AI

Process
Extinguishing systems
DI - DO

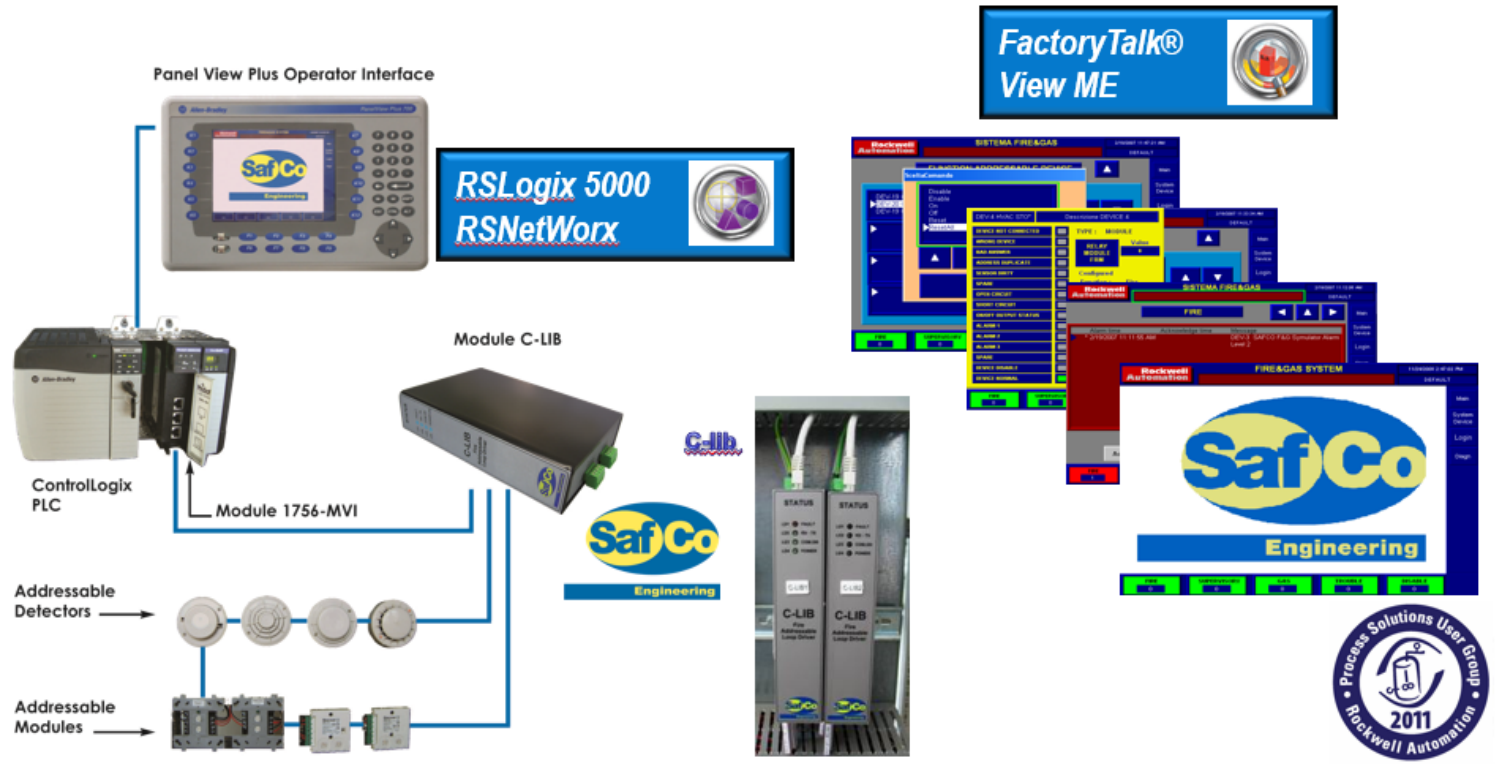
Building
Extinguishing systems
DI - DO

THE ADDRESSABLE FIRE DETECTION SYSTEM

Fire & Gas Networking

Safco provided an Integrated Unique Innovative Addressable Fire Detection System named C-LIB

SAFCO's C-LIB is the first addressable fire detection control panel fully integrated in a safety PLC platform. The C-LIB is designed to be configured as integrated card in the standard RSLogix 5000 Allen Bradley software platform and can be used in conjunction with all the Allen Bradley ControlLogix components, networking devices and IO cards, in order to realize a completely addressable and conventional Fire and Gas system.

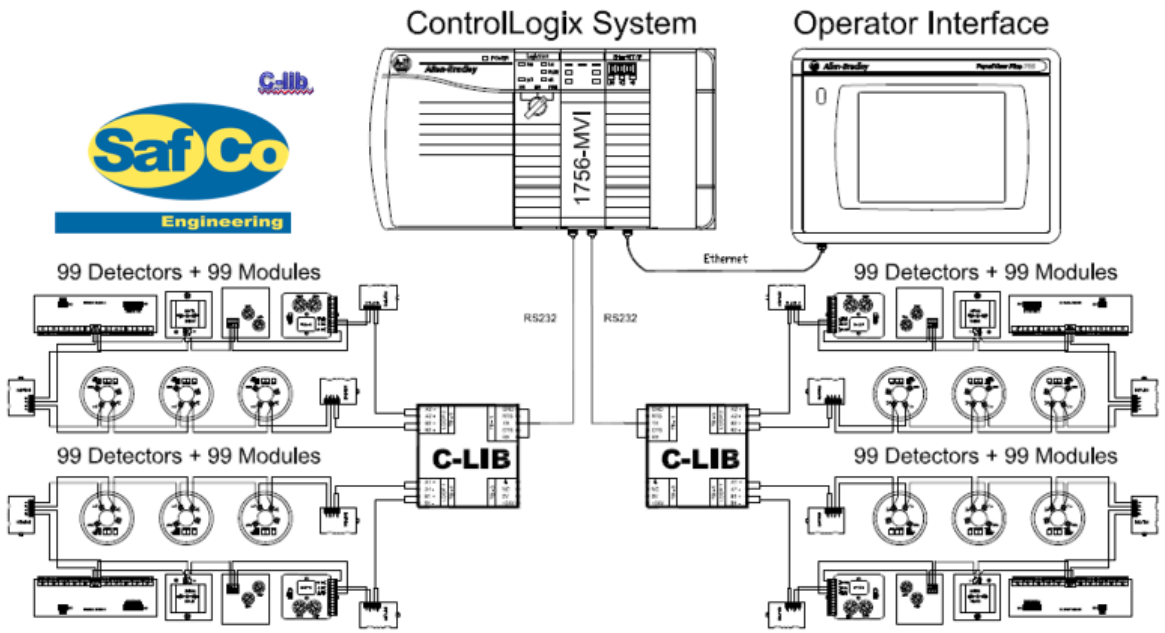


THE C-LIB MAIN FEATURE

Fire & Gas Networking

C-LIB is an addressable system fully integrated for building and process

- 2 Addressable isolated loops
- 99 detectors + 99 modules per loop
- 2 Cards per MVI controller
- 2000 mt loop length, furthest device 1300 mt
- Polling rate 30 millisecond per device
- 24Vdc powered
- TÜV certified according
- Fully programmable via standard RSLogix 5000
- On line replacement features

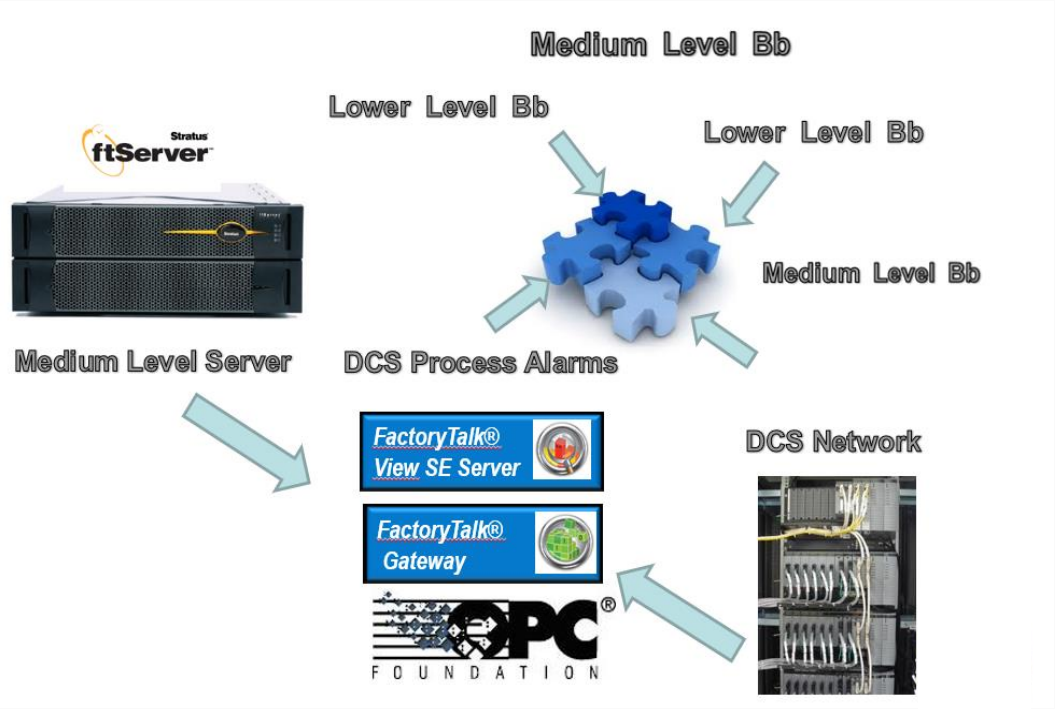


THE FINAL SAFCO INTEGRATED SYSTEM

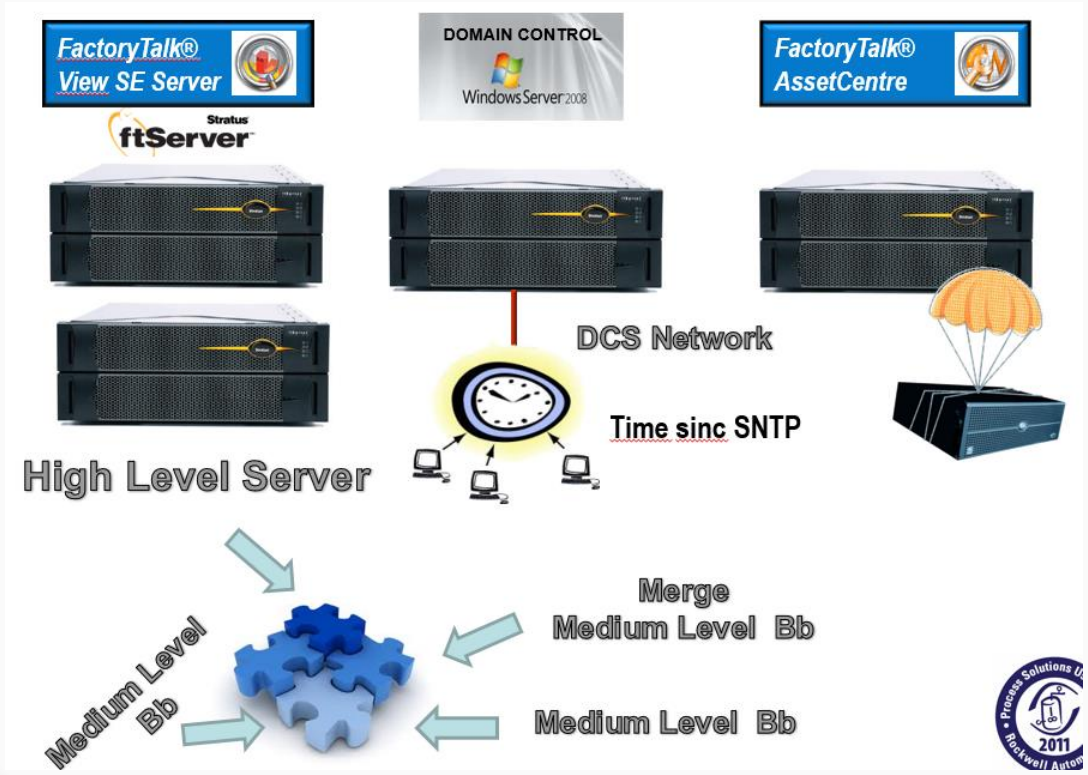
Fire & Gas Networking

Many Servers to control the entire Fire&Gas Detection & Alarm System

ML: OPC INTERFACE WITH DCS



HL: MAIN SERVER



THE FINAL NETWORK

The Project ended up with 93 Fire & Gas Panels to be installed in the refinery

Rockwell Automation

Allen-Bradley

SafCo Engineering

13000 DI
11000 DO
2000 AI
10000
ADDRESSABLE

Process Solutions User Group 2011 Rockwell Automation

PLANT AND SYSTEM EXTENSION

Fire & Gas Networking

Evaluating the customer need SafCo Engineering offered a System Extension

In 2014 due to the same refinery expansion, SafCo Engineering awarded the project for the Fire & Gas Detection System Extension.

The new job provided a new Server and a new Cyber Security policy

The New Cyber Security Policy has implied:

- Windows Server Update Services (WSUS)
- Antivirus Updates

2018

SLOWLESS ISSUE:

the 2009 Servers
are overload due to:
-increased I/O (new server expansion)
- WSUS
- Antivirus
This caused memory burden and slowdowns in the systems

THE PROJECT EVOLUTION

How the System has been evolving in the last ten years

Fire & Gas Networking

2009

SAFCO Engineering provided an **innovative** system fully based upon PLANT PAX Process Automation System and SAFCO intelligent fire panel (C-LIB)

MULTILEVEL NETWORK SERVER BASED

2014

SAFCO Engineering provided a **System Extension** based on server expansion and updating, fully pc intergrated

SERVER EXPANSION AND UPDATING

since 2018

the 2009 Servers are overload due to:
- increased I/O (new server expansion)
- WSUS
- Activate

This caused memory burden and slowdowns in the systems

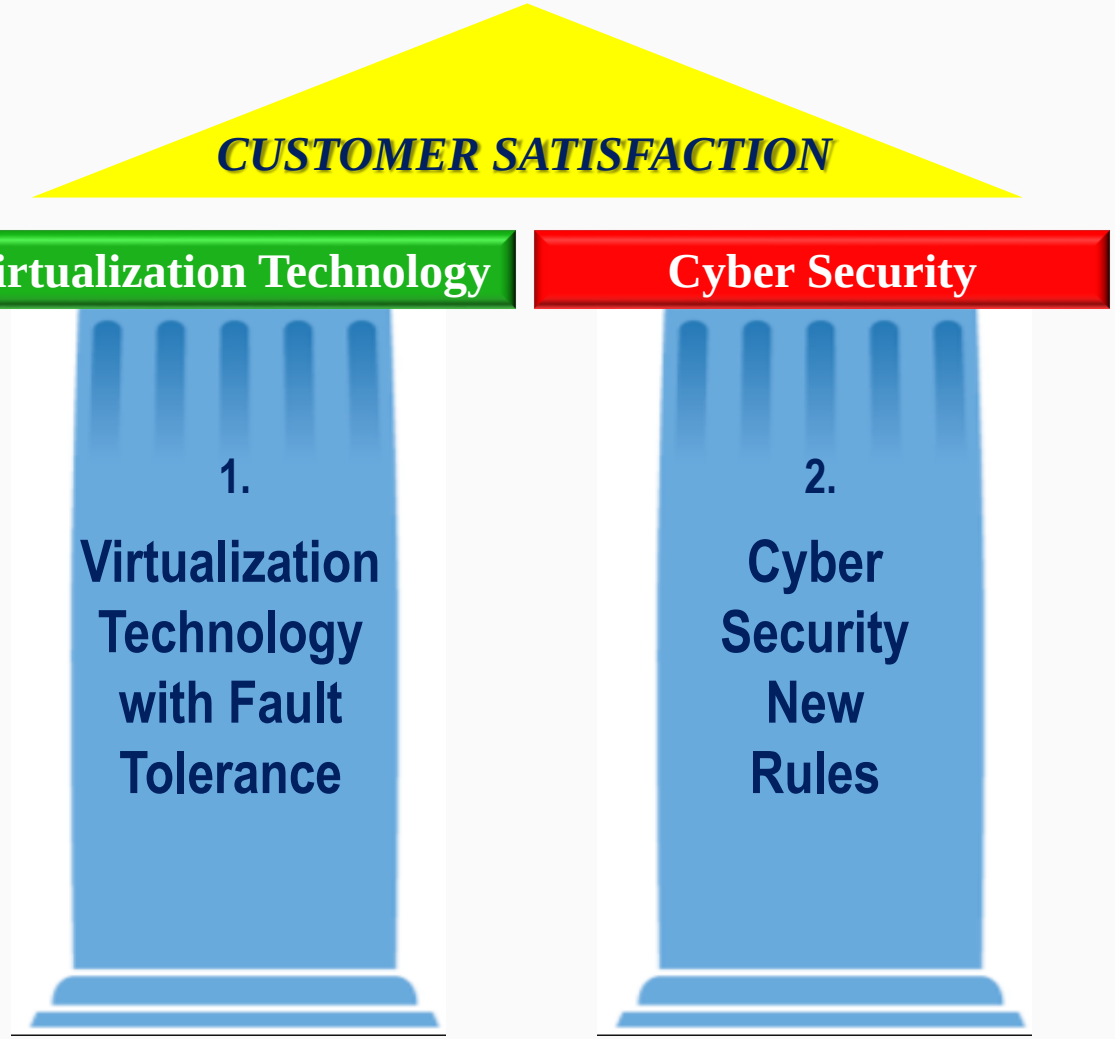
SLOWNESS ISSUE

Safco Engineering takes care of the problem and supports its top client with extra contract operations


Safco Engineering Innovative Solution

SAFCO INNOVATIVE SOLUTION PILLARS

The Safco Engineering Extra Contract Pillars for its Top Client Satisfaction

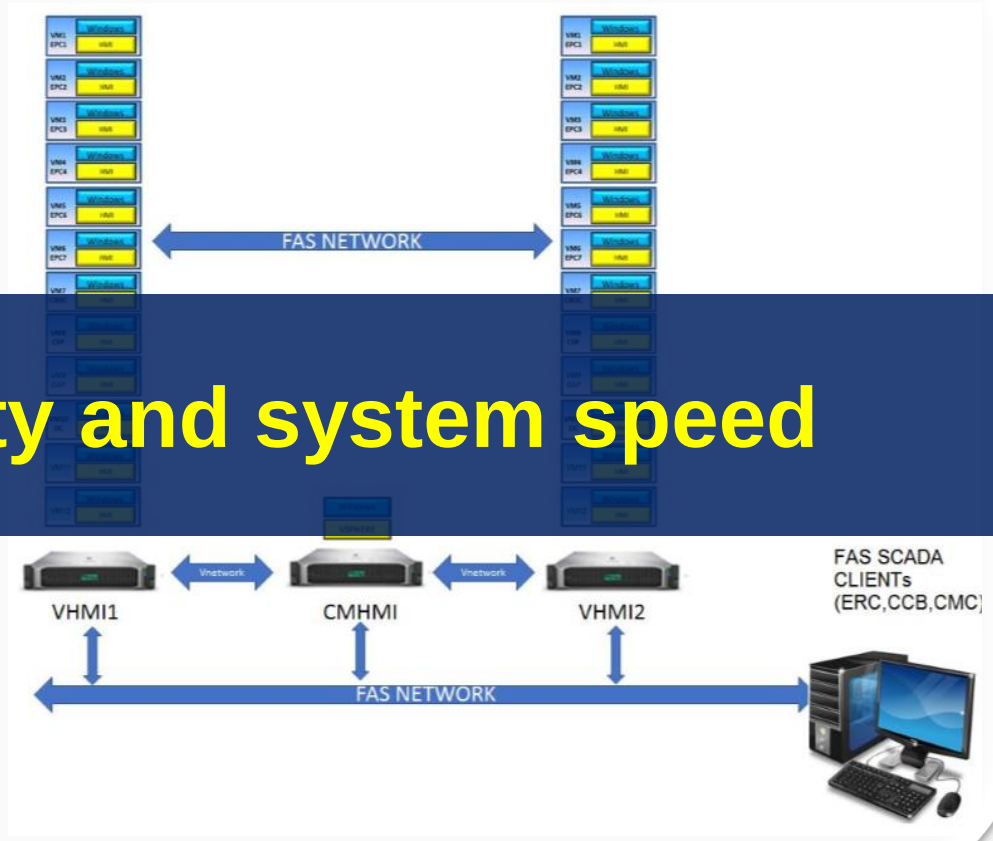


THE VIRTUALIZATION

Virtualization Technology

The new philosophy: a powerful hardware with several virtual machines for Fault Tolerance

- from five to two more powerful Servers + a central management HMI
- each Server host up to twelve Virtual machines
- most recent Window operating System
- DC integrated in the main system
- Fault Tolerance (FT):
  - Hardware → two redundant servers
    → DC automatically benefits of FT
  - Software → redundant and shared data



Maximum availability, reliability and system speed

SAFCO INNOVATIVE SOLUTION

Virtualization Technology

New server architectural configuration using advanced machines

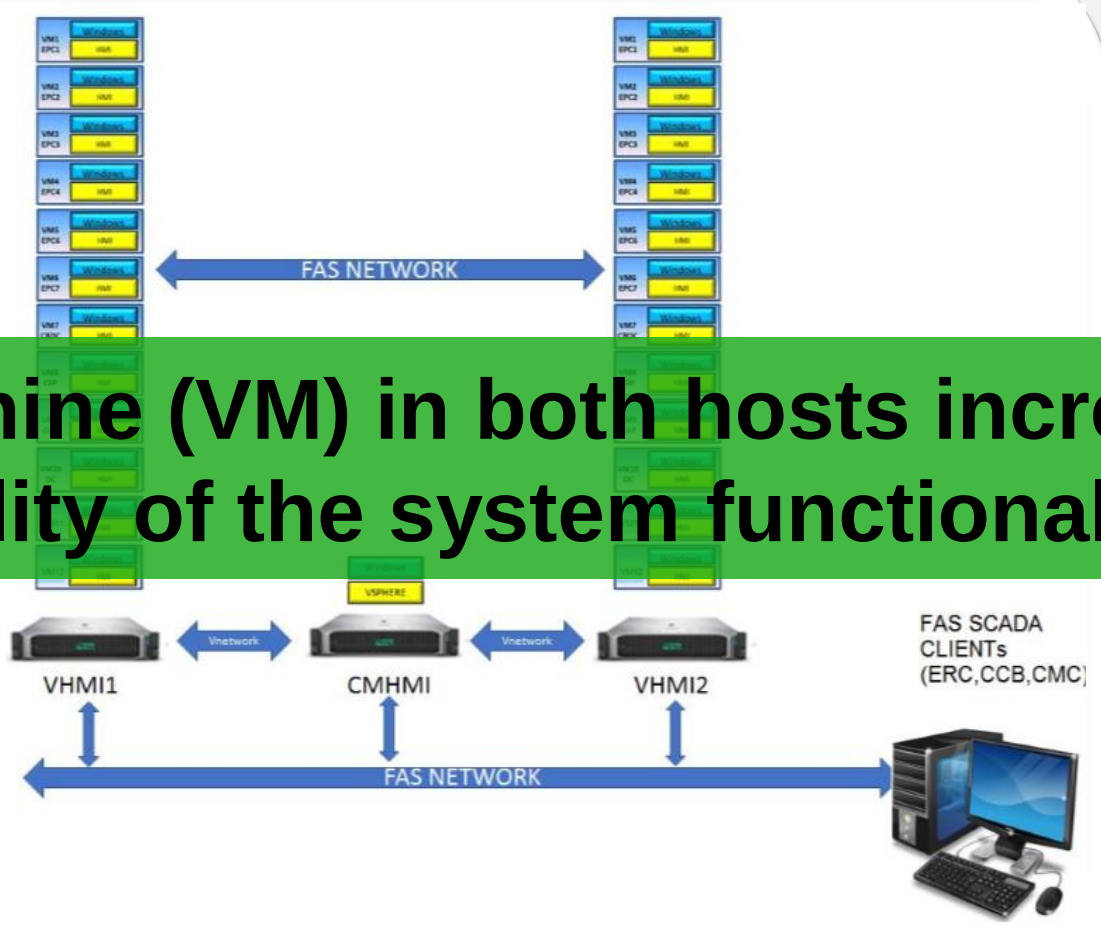
The new configuration architecture shall be composed of three server machines.

Two servers, VHMI1 (Virtual HMI1) and VHMI2 (Virtual HMI2), shall work in fully redundant configuration in term of hardware and software application installed in each machine and shall be dedicated to the SCADA applications used by operators to monitor the status of the fire alarm system signalization and visualization.

A third machine named CMHMI (Central Management HMI) shall be responsible of the management of the data shared and configured on VHMI1 and VHMI2.

All the machines shall be connected on the FAS network and shall be join to the domain of the FAS system in the refinery. Furthermore, the three new servers will be connected to an independent network for virtual machines management. New pair of managed switches shall be installed to realize the virtual management network.

On each VMHI a maximum number of twelve virtual machine shall be configured to run and the twelve virtual machines running on VHMI2 shall be the backup copy of the ones that run in VHMI1



Replicating the Virtual Machine (VM) in both hosts increase the availability and reliability of the system functionality

THE VSPHERE SOLUTION

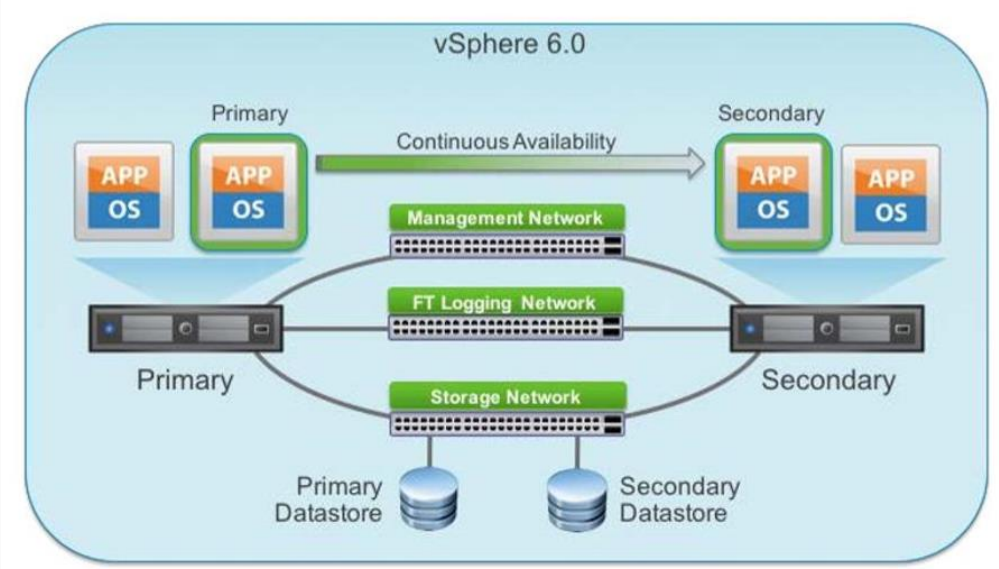
Guarantee of zero downtime and no disruption even in case of a complete host failure

vSphere FT enables a virtual machine to survive a physical server failure by creating an exact replica virtual machine on another host that can take over at the time of failure.

That means there is zero downtime, zero data loss, zero connection loss, continuous service availability, and complete transaction integrity.

vSphere FT works by continuously replicating an entire running virtual machine from one physical server to another. The result is that an FT-protected virtual machine has two replicas: the primary virtual machine and the secondary virtual machine, each running on distinct ESXi hosts. These replicas are logically identical —they represent a single virtual machine state and a single network identity, but they are physically distinct. Each replica has its own set of virtual machine files (including VMX and VMDK files), which vSphere FT automatically keeps in sync. When a physical server fails, one of the replicas will resume execution, and the virtual machine state, the network identity, and all active network connections for the virtual machine will be identical, ensuring a seamless failover process.

vSphere FT is made possible by four underlying technologies: storage, runtime state, network, and transparent failover



THE VSPHERE ARCHITECTURE

Four underlying technologies: storage, runtime state, network and transparent failover

Storage

vSphere FT ensures the storage of the primary and secondary virtual machines is always kept in sync.

When vSphere FT protection is enabled, an initial synchronization of the VMDKs happens using VMware vSphere Storage vMotion® to ensure the primary and secondary have the exact same disk state.

After this initial synchronization, vSphere FT will mirror VMDK write operations between the primary and secondary over the FT network to ensure the storage of the replicas continues to be identical.

Runtime State

vSphere FT ensures the runtime state of the two replicas is always identical.

It does this by continuously capturing the active memory and precise execution state of the virtual machine, and rapidly transferring them over a high-speed network, allowing the virtual machine to instantaneously switch from running on the primary ESXi host to the secondary ESXi host whenever a failure occurs.

Network

The networks being used by the virtual machine are also virtualized by the underlying ESXi host, ensuring that even after a failover, the virtual machine identity and network connections are preserved.

Since vSphere FT preserves the storage, the precise execution state, the network identity, and the active network connections, the result is zero downtime and no disruption to users should an ESXi host failure occur.

Transparent Failover

vSphere FT ensures that the primary always agrees with the secondary about the state of the virtual machine. This is achieved by holding externally visible output from the virtual machine, and only releasing it when an acknowledgement is made from the secondary affirming that the state of the two virtual machines is consistent (for the purposes of vSphere FT, externally visible output is network transmissions).

The cost for maintaining this zero data loss consistency is that network transmissions from the virtual machine are delayed until the two virtual machines are in a consistent state.

THE FACTORY TALK VIEW

Virtualization Technology

The software that can involve multiple users, clients and servers over a network

FactoryTalk View SE is the integrated software package for developing and running HMI applications that can involve multiple users, clients and servers, distributed over a network.

Factory Talk View including FactoryTalk Services Platform and Data Communication products such as FactoryTalk Linx shall be installed in VHMI1 and VHMI2 virtual machines.

This means that the Factory Talk network directory sharing all the data base information and communication resources shall be assigned to one of virtual machine located in VHMI1 and its replicant in VHMI2.

Each virtual machine shall have its tag data base server and plant graphic pages covering EPC areas.

FactoryTalk Linx shall be installed and configured as communication server for EPCs area in each virtual machine.


CYBER SECURITY

CYBER SECURITY

Cyber Security

The new approach to reduce the risks of being attacked externally

Being the FAS network and the Vsphere Management isolated and not exposed to the Internet, the possibility to be attacked externally is drastically reduced

Fas system network is considered segregate network and isolate because the only interface with PWN network is secured by Third Part Firewall (Tofino)

CYBER SECURITY REGULATIONS

Cyber Security

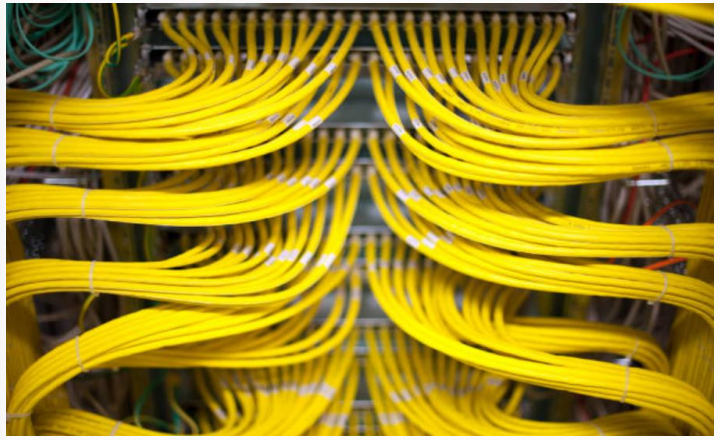
The new rules to avoid the risks of being attacked externally

- On the **Domain Controller** shall be installed **agent antivirus** and every antivirus **update** shall be load manually and **validated** by Rockwell Software Technical Support Web Site.
- **Not Automatic Windows update operating system and paths capability:** the **update** compatibility must be **validated and tested** separately before being installed
- The **unused network ports** in all network devices (Server and ethernet switches) shall be **power off** (hardening).
- All the **unused media drivers** like USB ports and CD drivers shall be disabled, only authorized personal shall unlock the media device in order to be used for maintenance activities. **Rules and privileges** to lock/unlock media drivers shall be configured in the **FAS Domain Controller**.
- **Access control to the servers and client machines** shall be permitted to the authorized users by configuring them in the **FAS Domain controller** with their access policy.

THE EVOLUTION

The technology evolves and Safco Engineering is always on the edge in solving his clients needs

Fire & Gas Networking



Virtualization Technology

Cyber Security

We are looking forward to serving your project needs.

Contact us

www.safcoengineering.com

Safco Engineering S.p.A.
Via Caduti del Lavoro, 10/A
20096 Pioltello (MI)
Tel. +39 02 95327396 – Fax +39 02 95327086
Emai: info@safcoengineering.com

Safco Engineering S.R.L – Abu Dhabi
Khalifa Street - ADNIC Building, 9th Floor, AYA Business Centers LLC P.O. Box 27212 - Abu Dhabi - U.A.E
Tel. +971(2) 418 9100- Fax +971(2) 666 1863
Email: safco.uae@safcoengineering.com

Safco Engineering S.R.L – Asia Pacific
Nonhyun-Dong 267-18, Gangnam-Gu, Seoul, Korea
Tel. +82 10 4453 2334
Email: sw.lee@safcoengineering.com

We care for Your Safety

We are waiting for delivering the best solution to your needs