PcVue Architectures & Deployment

Last update :	September 2022
Revision :	11
Content :	Describe the architectures and deployment solutions for PcVue
Confidentiality :	Public

Content

1. Overview

This document explains the options for deploying the Supervisor.
Deployment is the process of allocating roles to workstations and servers to fulfill the system requirements in a given physical network architecture.
For the purpose of this topic we will consider that the Supervisor has the following main functions:

• **Data acquisition** - The collection of real-time data, representing real-world or calculated values, using a communication protocol such as Modbus, OPC...
• **Historical data recording** - The recording of real-time data so that it can be accessed at a later time either by the Supervisor itself or a third party application.
• **Alarms** - Alarm generation and management.
• **HMI** - Human Machine Interface. The graphical interface that is the presentation layer and enables operators to interact with the monitored system.
• **Inter-station networking**. The mechanism by which the Supervisor distributes real-time and historical data between stations in networked architectures.
• **Web Server extensions**. A set of components used to interface the Supervisor's core architecture with web clients.
• **Interface to 3rd party systems** - Such as CMMS, GIS, ERP, MES...

Functions and roles allocation cannot be achieved independently from the licenses. For more information about licensing, please contact your local sales representative.

1.1 Architectures

The typical architectures are as follows:

• **Standalone** - All SCADA functions are incorporated into a single station.

• **Multi-station architecture** - The SCADA functions span across two or more stations in a client/server architecture.

• **High availability architecture** - The SCADA functions and roles are distributed to offer better resilience and scalability. Multi-station deployment includes the following particular scenarios:

- **Data acquisition redundancy** - Two or more stations are configured as redundant (hot standby).
- **Historical data redundancy** - Two or more stations are configured as redundant (hot standby).
- **Mutualized servers**.

• **Three-level architecture** - Using one or more stations as a gateway

• **Engineering station** with version management

• **Web & mobile** - Web backend server and web-based and mobile clients.

1.2 Roles

The architectures above require allocation of the following roles:

• **Data acquisition**
- Communication with field devices,
- Real time data and alarm production,
- Serves real time data and alarms to other stations.

• **Historical data**
- Consume real time data and alarms produced by other stations,
- Handles data storage, the recording and replay of historical data,
- Manages connections to RDBMS,
- Serves historical data to other stations.

• **Web backend server**
- Consume real time data and alarms produced by other stations,
- Consume historical data produced by other stations,

- Manages the interface with IIS,
- Serves Web clients including WebVue clients, TouchVue clients, the WebScheduler and the Web Services Toolkit clients

• **Gateway**
  - For the secure transfer of data between 2 networks
  - Consume real time data, alarms and historical data produced by other stations on one network,
  - Serves real time data, alarms and historical data to stations on another network.

• **HMI**
  - Display mimics, graphics, alarm viewer, log viewer, trend viewer... to the user.

Depending on the combination of roles, the Supervisor's stations are better deployed on a desktop operating system or a server operating system.

1.3 Architecture building blocks

1.3.1 Legend


HTML5


Firewall


Web backend Server


Proprietary archives


HDS archives


Stand alone


PcVue network access

Server stations

Client stations


Central version folder


FrontVue


PcVue instance

Building blocks	Typical roles	Typical deployment mode
Standalone station 	• Data Acquisition • Historical data • HMI • Does not have the capability to exchange data with other stations	• As a Desktop Application • Under a desktop OS
SCADA station 	• Data Acquisition • Historical data • HMI	• As a Desktop Application if it requires an HMI • Under a desktop OS Or • As a Windows Service if an HMI is not required • Under a server OS
Data acquisition server 	• Data Acquisition	• As a Windows Service • Under a server OS
Client station 	• HMI	• As a Desktop Application • Under a desktop OS • Or with a server OS hosting Remote Desktop Services combined with lightweight terminals used as operator workstations
Historical data server 	• Historical data	• As a Windows Service • Under a server OS
Web server 	• Web server	• As a Windows Service • Under a server OS
Web clients 	• Remote monitoring and control over the Internet or Intranet. • WebVue clients and TouchVue clients.	• Using a Web browser or a Web App • On a desktop PC or a mobile device

Engineering station

- Depending on the architecture and project design, an engineering station can have very different roles, ranging from those of a data acquisition server (for testing communication with field devices), to archive server or just an HMI workstation (to design mimics).
- Project development and maintenance.
- Project and libraries version management.
- Interoperability with third-party generation tools.

- As a Desktop Application
- Under a desktop OS

2. Architectures

This topic describes the most common base architectures. There are many variations to fit system requirements in term of:

- Number of users
- Type and number of operator stations (HMI)
- Availability
- Flexibility
- Scalability
- Resilience
- Maintenance and application lifecycle management

Please contact the technical support for more information.

2.1 Stand-alone station

- ✓ The simplest architecture
- ✓ To monitor and control your process from a single “all-in-one” station
- ✓ All performances of a PcVue station for a stand-alone architecture

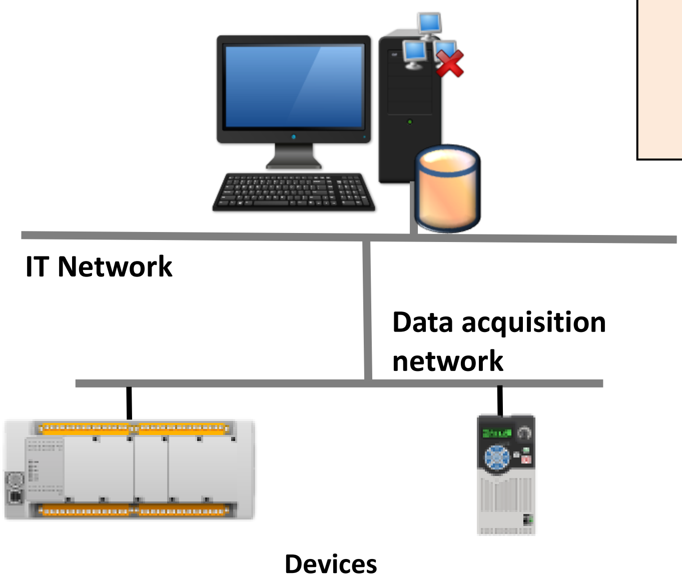


Figure 1 - Stand-alone station

Standalone stations are usually operator panels, it is the simplest architecture with all functions and roles integrated into a single station.

In a traditional single-user configuration, PcVue monitors and/or controls all devices on the industrial network and also handles user requests. PcVue can support some tens of thousands of variables on a single station.
The PcVue single station is an all-in-one standalone HMI station to monitor and control the process using the standard features of PcVue:

- ✓ Data acquisition,
- ✓ Real-time database,
- ✓ HMI,
- ✓ Archiving,
- ✓ Alarms and logs,
- ✓ Trends,
- ✓ Data processing, reporting
- ✓ Users management

2.2 Multi-station

- ✓ The simplest multi stations architecture
- ✓ The process is monitored from several remote user stations
- ✓ Data processing network load optimized

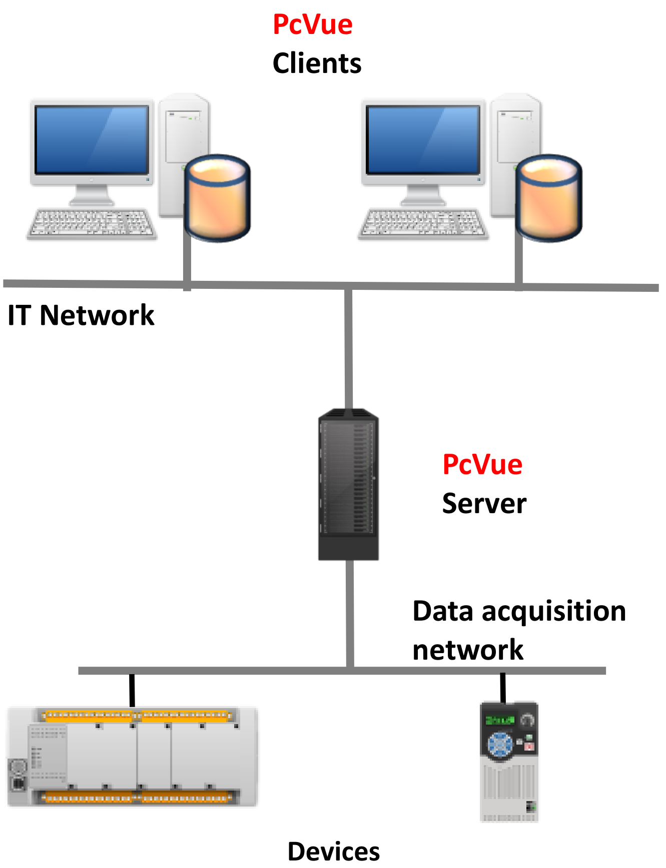


Figure 2 - Multi-station

The simplest client/server architecture, for applications that require several user stations with a single connection to the industrial network.
The server is a data source (producer) that communicates with the devices and broadcasts data to the client (or consumer) stations. Communication among the PcVue stations works asynchronously and transmits the data in packets using the PcVue TCP/IP messaging.
The server station can be a full user station or a data acquisition server only. It performs all of the data processing for the application. The historical data can be on server side only, or local to each client station.

A client can connect to a server located in another geographical area via a connection using any media supporting TCP/IP with sufficient capacity including private telephone line, or even satellite link.
A usual variation is to separate Data Acquisition and Historical Data production on 2 different servers, or to have clients produce historical data locally.

2.3 Multi-station with a Remote Desktop Server for deploying client stations

- ✓ To reduce the administration effort and costs
- ✓ Low-cost thin hardware clients
- ✓ Installation free on thin clients

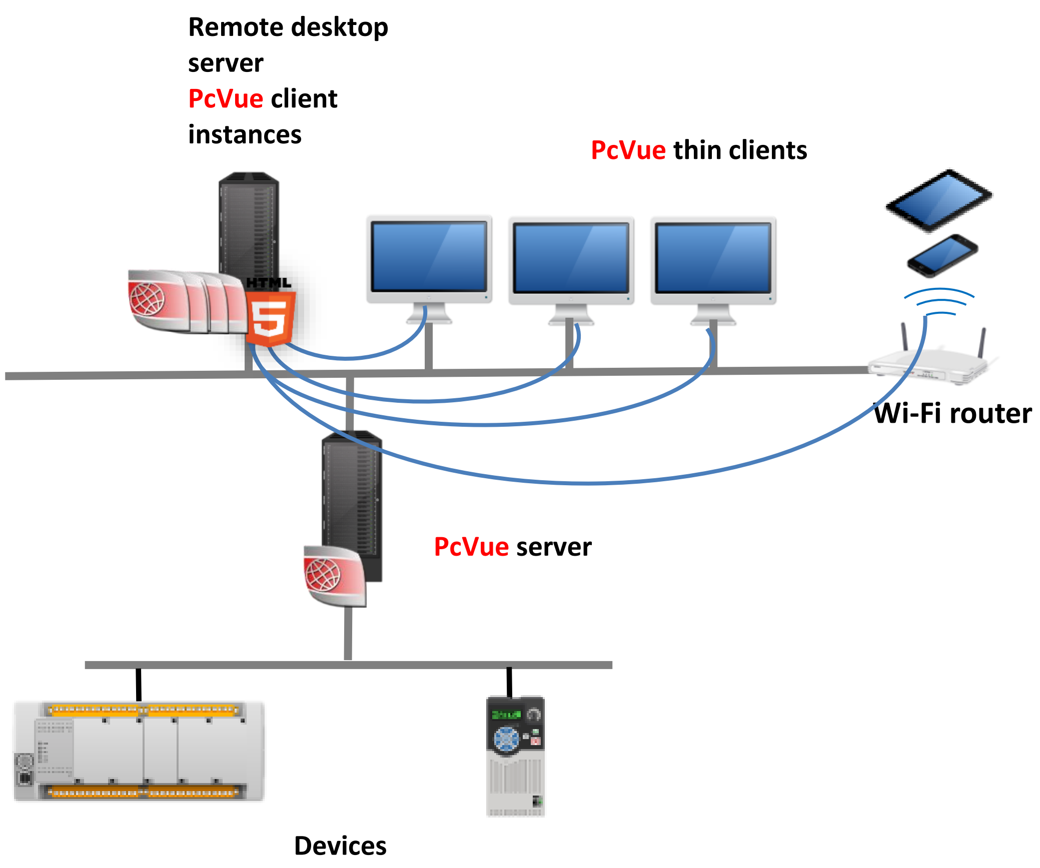


Figure 3 - Remote desktop architecture

Windows Server, when configured with Remote Desktop Services, allows several users to concurrently use the resources of a single server and to execute applications installed on the server. A user interacts with applications using a thin client (also known as terminal) connected to the server using a network. The process of a user connected to Windows Server in this manner is called a Remote Desktop Session and uses a standard known as the Remote Desktop Protocol (RDP). Thin clients (including Wyse Thin Computing terminals under Linux or Unix) use RDP client software for managing the RDP.

In addition to running sessions using a remote desktop, Windows Server also runs a session using the local monitor, keyboard and mouse. This is referred to as the local session (or sometimes as a console session or interactive session).

When running the Supervisor on a RD Session Host server, an instance of the Supervisor can be run from each Remote Desktop Session and/or from the local session. Only a single copy of the Supervisor is installed.

This architecture, from a Supervisor's networking point of view is the same as the previous one except that as a way to rationalize the deployment of client station, RDS and lightweight terminals are used.

In this example a PcVue Client is installed on a station with Windows Server operating as a Remote Desktop Server (RDS).

This station is a RD Session Host server and hosts PcVue client instances. Users can open a Remote Desktop Session from any thin client and run a PcVue client instance. An HTML5 interface on the server allows any thin client equipped with a **HTML5**-compliant Web browser to access the PcVue applications through an RDS instance.

The PcVue Server, when there is only one, can also reside on the RD Session Host server.
The RD Session Host server must be configured to host multiple Client instances for supporting the required number of simultaneous sessions. The thin clients do not require any specific installation, which facilitates on-site deployment of the application.

2.4 High availability

- ✓ Very high level of security and system/data availability
- ✓ Secure Client-Server setup with dual networks
- ✓ Several user's stations
- ✓ Data processing and field networks data load optimized

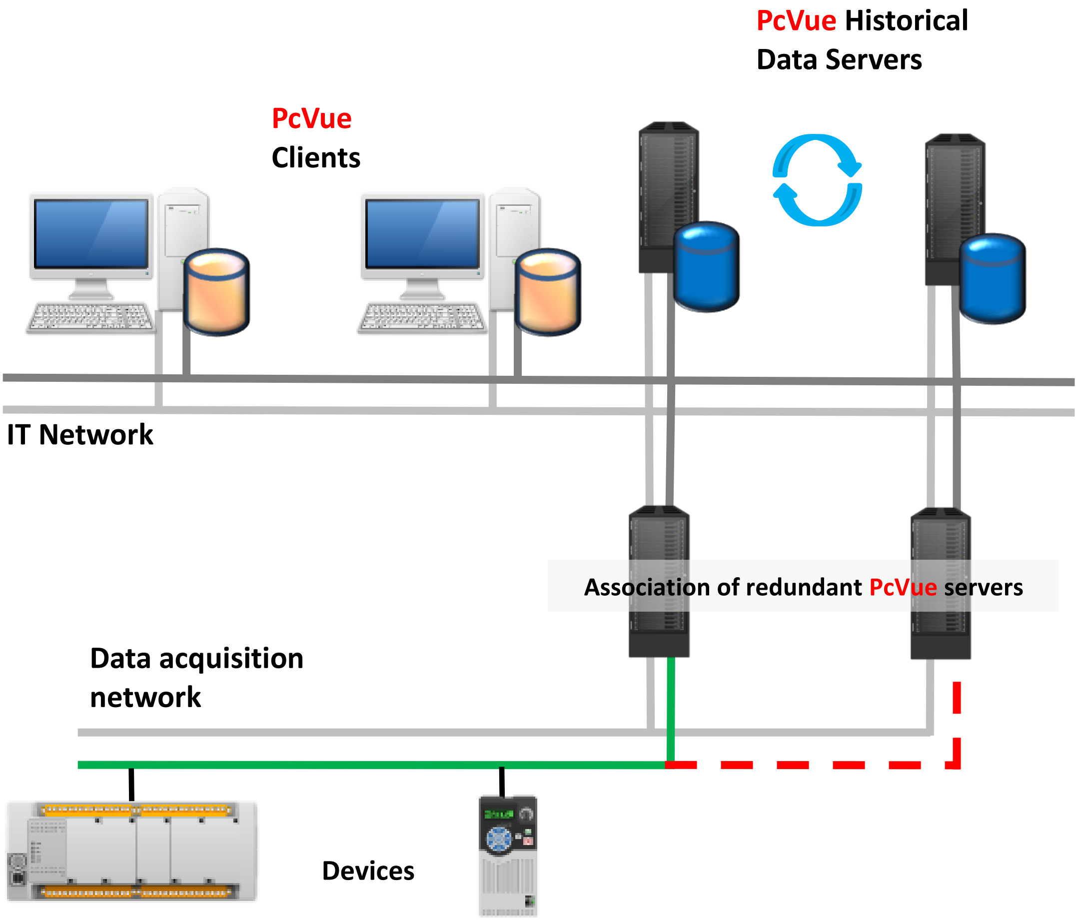


Figure 4 - High availability architecture

When a higher availability and resilience are required, this architecture, more distributed, brings redundancy and roles separation.
It is similar to the multi-station architecture but with data acquisition server and historical data server separation and redundancy.
The inter-station network (LAN and/or WAN) can be duplicated, as can the field network. There are then two independent paths between any client station and the data sources. Each PcVue client station maintains two connections with each server

station and will attempt to switch between servers only when both of these connections are inoperable.
On an Industrial Ethernet network, PcVue can manage both communication media redundancy and device-level redundancy.
Each station can archive the data to improve the historical data availability.
A usual variation is to also include a Web Server and Web clients, thus combining permanent operator's seats and one-off user connections.

2.4.1 Real-time redundancy

The servers are dedicated to the acquisition on the PLCs and update the information (database) of the client stations in real time. The client stations have graphical interfaces for monitoring and control the process.
The 2 servers are redundant between them and feed the client stations of the site.

2.4.2 Single Active Acquisition Server Mode

Servers operate in Single Active Acquisition Server mode. The server that communicates with the industrial network is called "active". The other server is called "passive". Only the active server manages the communications on the PLC systems, feeds the client stations and synchronizes the passive server.
In the event of a failure of the active server, the passive server activates its communications with the acquisition systems and feeds the client stations. The switchover is done hot and completely seamless to the operators.
When starting a server, there are two possible scenarios:

- The other server does not work. The new server initiates communication on the industrial network to refresh its Equipment variables and becomes the active server. All Clients in the network are automatically subscribed to.
- The other server is already running and active. The new server automatically becomes passive and synchronizes itself to the active server.

When a passive server becomes active, communication resumption on the industrial network is immediate, which makes the new active server instantly operational.
The client stations are fed on an event and automatic basis by the active server at time T. For the operator access to information (control / command / acknowledgment / archive ...) is identical from any station; there is complete transparency on the origin of the data whatever the state of the network. Depending on the user profiles, it is possible from any client workstation to access all or part of the site information.
From any station, it is possible to know the status of all network stations and communications on the acquisition systems. The system provides a complete architecture diagram with real-time visualization of the PLCs and supervisors connected to it.

The system allows for maintenance issues, and according to authorization, to act on the state of the network (for example: to force a passive server to become active).

2.4.3 Archives redundancy

2.4.3.1 Mode with 2 synchronized archive databases

The 2 servers are also history servers in order to log information in parallel on 2 separate SQLServer Relational Databases. Both servers record the same information at the same time.
Previous configurable date range information is automatically purged. In this way, the size of the database is controlled, which guarantees the best possible access times compared to the desired "depth" of history.
Purged records can be retrieved from ASCII files to be "backed up" if necessary.
Periodically an automatic consolidation of the missing information is made to manage the cases of stops (breakdown or maintenance). This consolidation is done crosswise: the 1st server retrieves its missing histories on the 2nd server and vice versa. At the end of the consolidation the Relational Databases are identical.
Consolidation runs in parallel with standard accesses on the Base (read or write) and communications.
Each Supervisory Client transparently accesses the history of the active server and thus has a continuous archive from any client station.

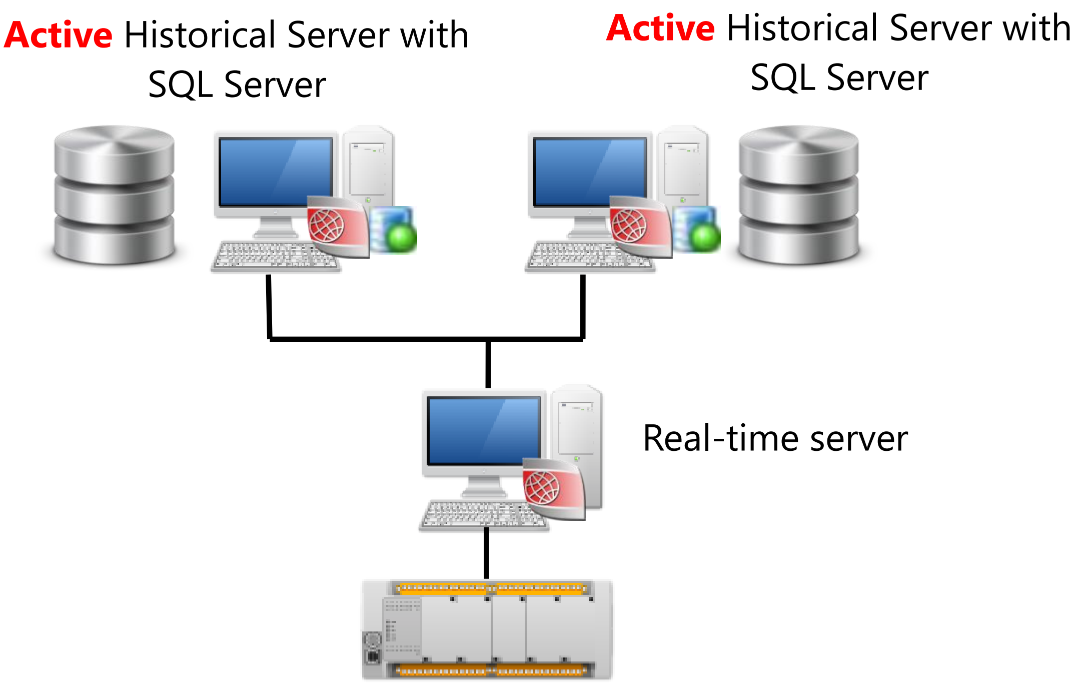


Figure 5 – 2 synchronized active SQL server

2.4.3.2 Mode with only 1 archive database

The principle is to have a machine (preferably Windows Server type) that hosts the database and the SQL Server engine and is different from the two real-time servers PcVue.
Following the single active server principle previously described, only the active PcVue server stores the information in the database. So, in all cases there is always at least one server that archives the information.
If the server hosting the database fails, the active PcVue server stores the information locally. When the connection to the SQL Server database returns, the active server transfers the locally generated archives to the central database.
All of its integrated functions ensure archival continuity from the moment at least one of the PcVue servers is available.

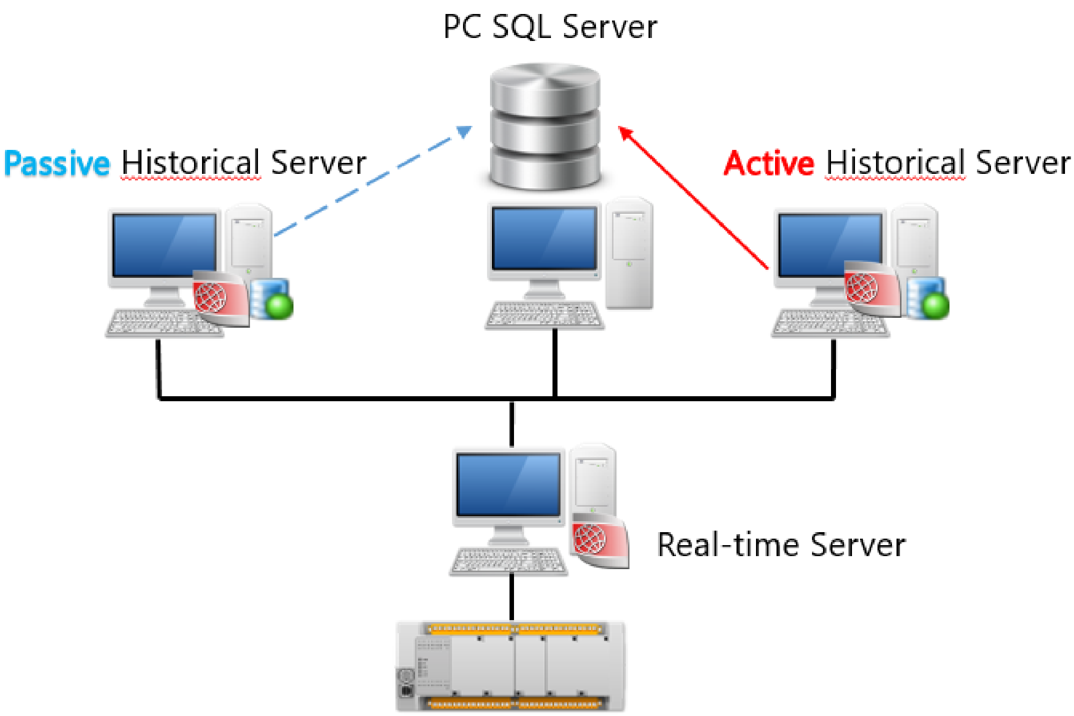


Figure 6 – Single active SQL server

2.4.4 RDS redundant architecture

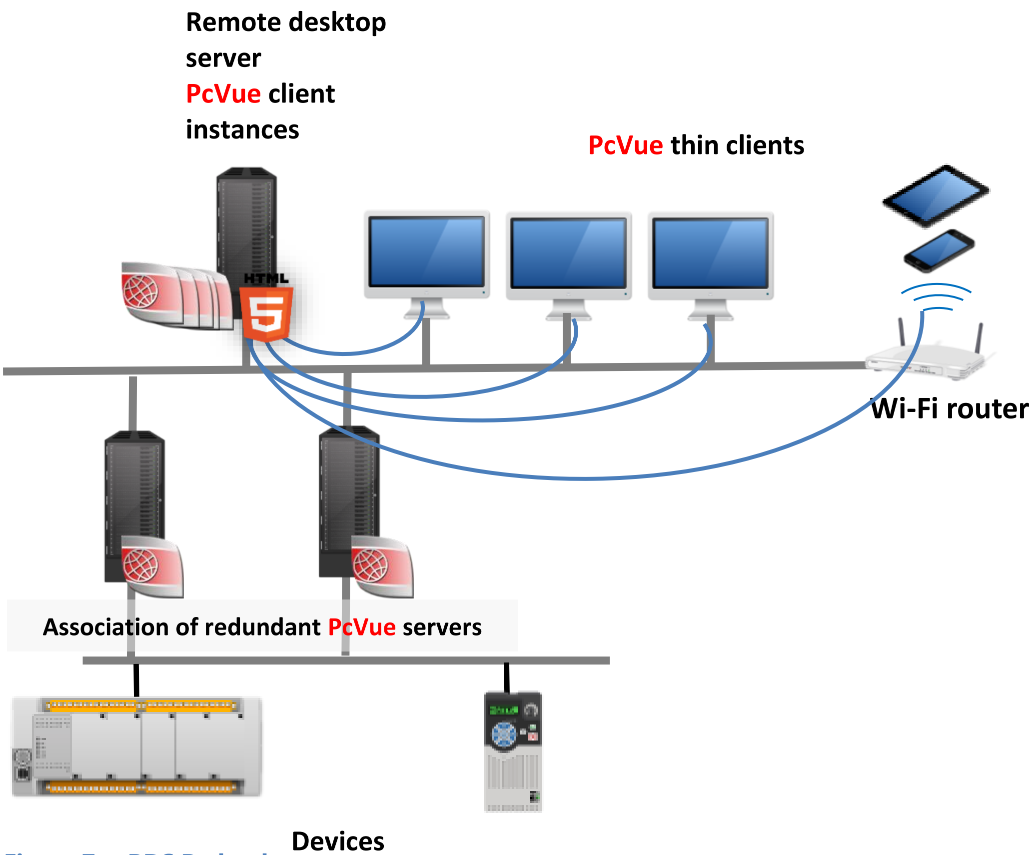


Figure 7 – RDS Redundancy

In this architecture, redundancy is provided by the 2 acquisition server stations.

Remote access is provided by a Windows server workstation with the RDS role.

Failover is automatically managed by PcVue at the level of the acquisition servers.

2.5 Mutualized server

- ✓ Optimized redundant architecture to monitor and control multiple processes
- ✓ Reduce deployment and maintenance effort

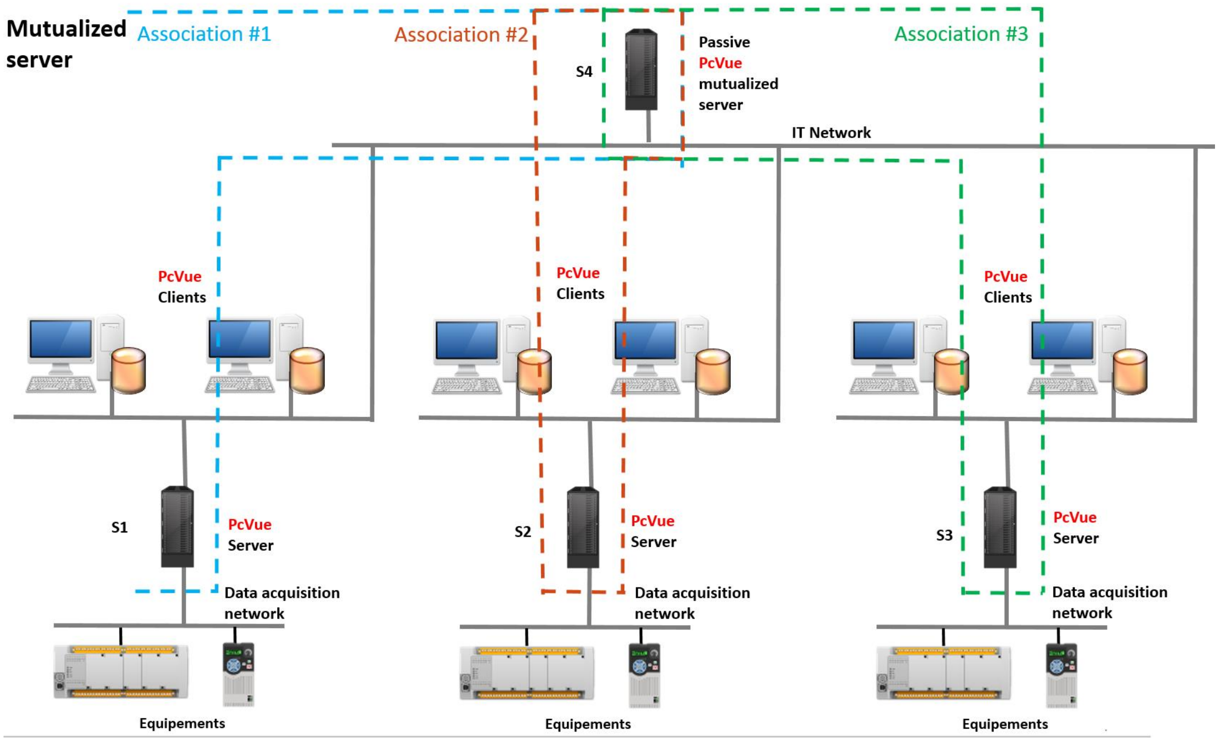


Figure 8 - Mutualized server architecture

The mutualized architecture is an interesting variation of the high-availability. When you have to monitor and control multiple processes, production lines, plants, buildings, sites… and can benefit from a reliable network, you can set up a high-end server that will be used as the standby server for multiple other zones. By mutualizing the standby server, you achieve redundancy and availability while minimizing the overhead of deploying and maintaining a fully duplicated set of servers.

This kind of architecture may not be suitable with any protocols. Please contact your technical support for more information.

2.6 Multi-level

When network segmentation is a concern, a gateway can be added to the architecture.
Such an architecture is useful when, for example, the system spans over a Wide Area Network, or when data consumers (client stations or data repository) are located in a less-trusted network.
Such a gateway can be deployed in a DMZ, and if necessary gateways can be redundant.

In a distributed architecture each station may be a data source (producer) for some variables and a consumer for some others. Moreover, some stations may act as data concentrators for a central control room located in another geographical area.
PcVue allows the development and deployment of multi-server/multi-client applications whereby the various server associations are configured to allow some of them to primarily retrieve information from devices, and others from other servers (as client stations do).
Central servers collect only a subset of all the information, allowing efficient monitoring of the devices from the central control room.

2.6.1 Multi-level: implementation #1

- ✓ For very large scale applications and geographically widely distributed system
- ✓ Several levels of control
- ✓ Very flexible

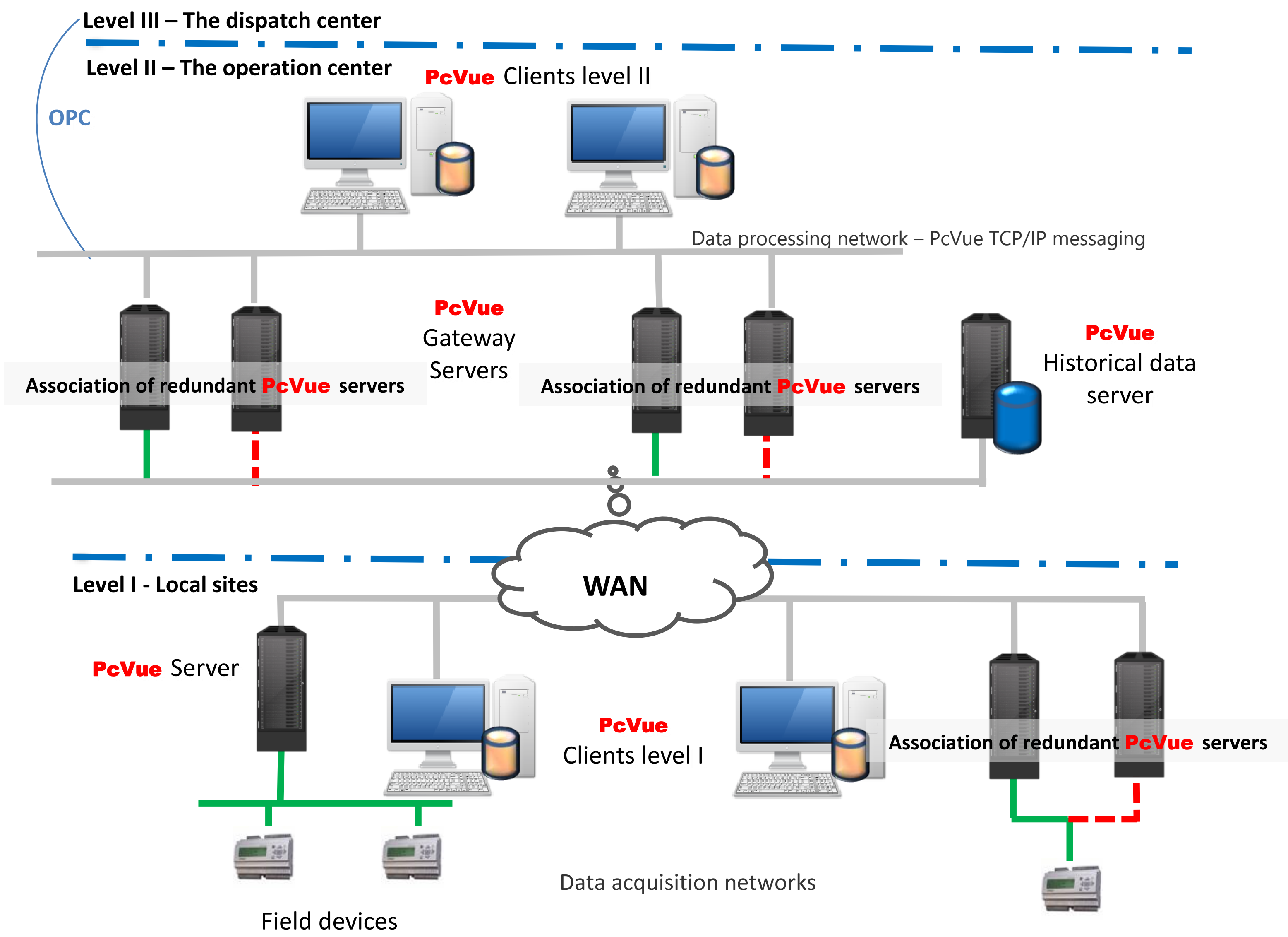


Figure 9 - Multi level architecture #1

The **level I – Local sites** is composed of PcVue stations widely distributed getting the data from the field devices and making the data available to the level II through a Wide Aera Network with satellite connection for example.

The **Level II – The operation center** is the core of the architecture with redundant associations of PcVue servers to centralize the data from different stations from level I. Each association of server handles thousands of real time variables and archives the higher critical variable locally.
A pair of servers can also be dedicated to archive the low critical data to a DBMS.
The Client stations connected to the server stations are used as operation and engineering consoles and help the operators to monitor and control the variables from any sites (Real time, alarms...).
The **level III – The dispatch center** is the highest level of the architecture. It receives the main data unified from the level II through an OPC connection.

2.6.2 Multi-level: implementation #2

- ✓ For geographically widely distributed system
- ✓ Several levels of control
- ✓ For **very large amount of data**/high growth rate projects
- ✓ Very flexible

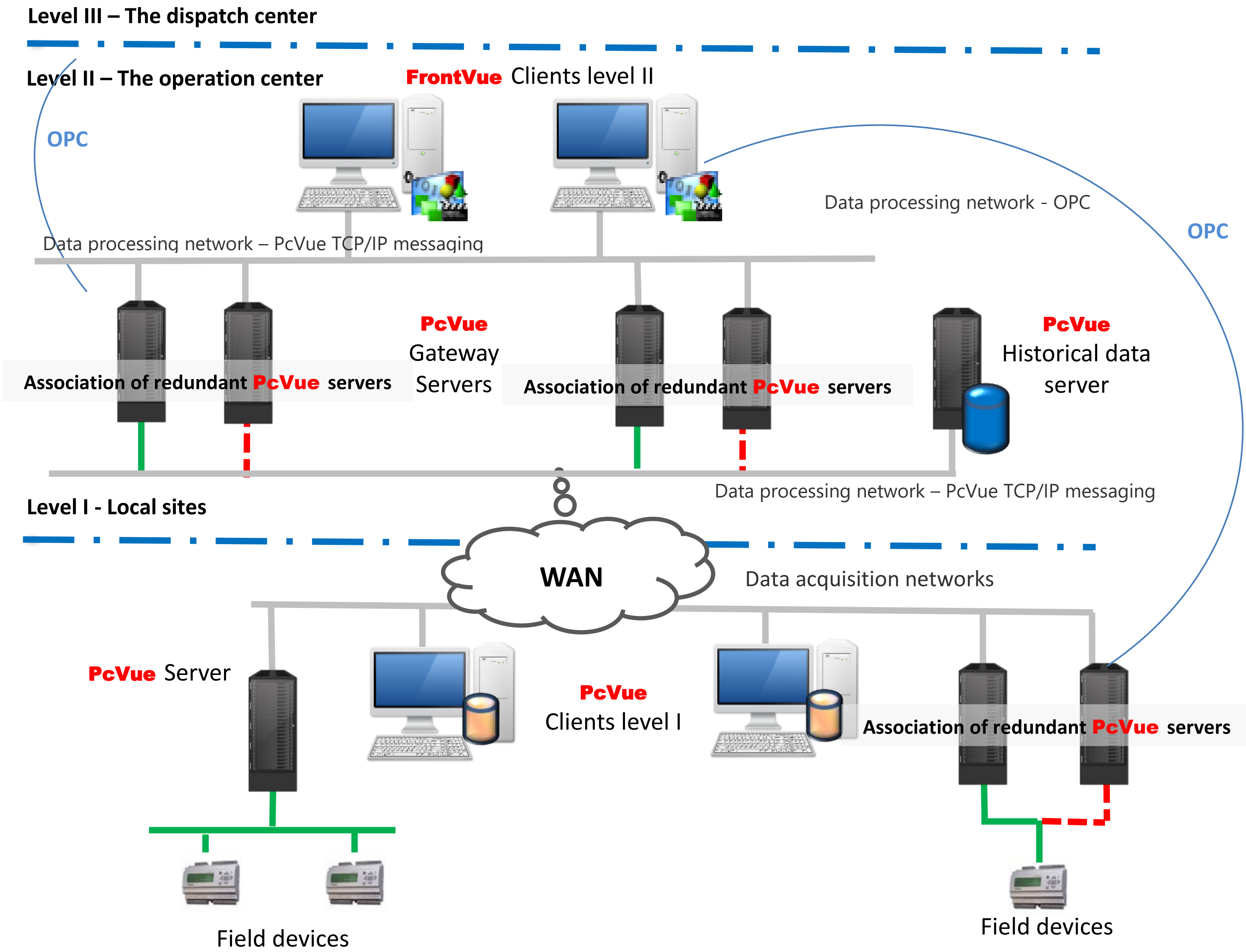


Figure 10 - Multi-level architectures #2

When the application becomes bigger (over 300 000 variables), it makes sense to optimize the architecture replacing the rich PcVue clients with the lighter FrontVue HMI clients to insure the scalability of the system.

FrontVue is a very lightweight OPC-based HMI client with no embedded treatment or archives. Connected to PcVue as an OPC client, it gets and allows monitoring and controlling real time data and can display alarms and historical data that are managed on PcVue side.

FrontVue refreshes only the data displayed which allows to:

- minimize application start-up time on clients
- dramatically reduce the data load on the network

FrontVue can connect on several OPC servers which allows to

- connect to remote local servers for retrieving detailed information from any specific device.
- display concatenated events from several PcVue servers to present a single/unique list to the operator in the alarms/logs viewers.

2.7 CLOUD Architectures

2.7.1 Architecture #1: Cloud interoperability

- ✓ Seamlessly connect cloud database
- ✓ For sharing data from PcVue to third party systems such as ERP, SCADA,...
- ✓ For getting data from existing devices such as IoT to PcVue

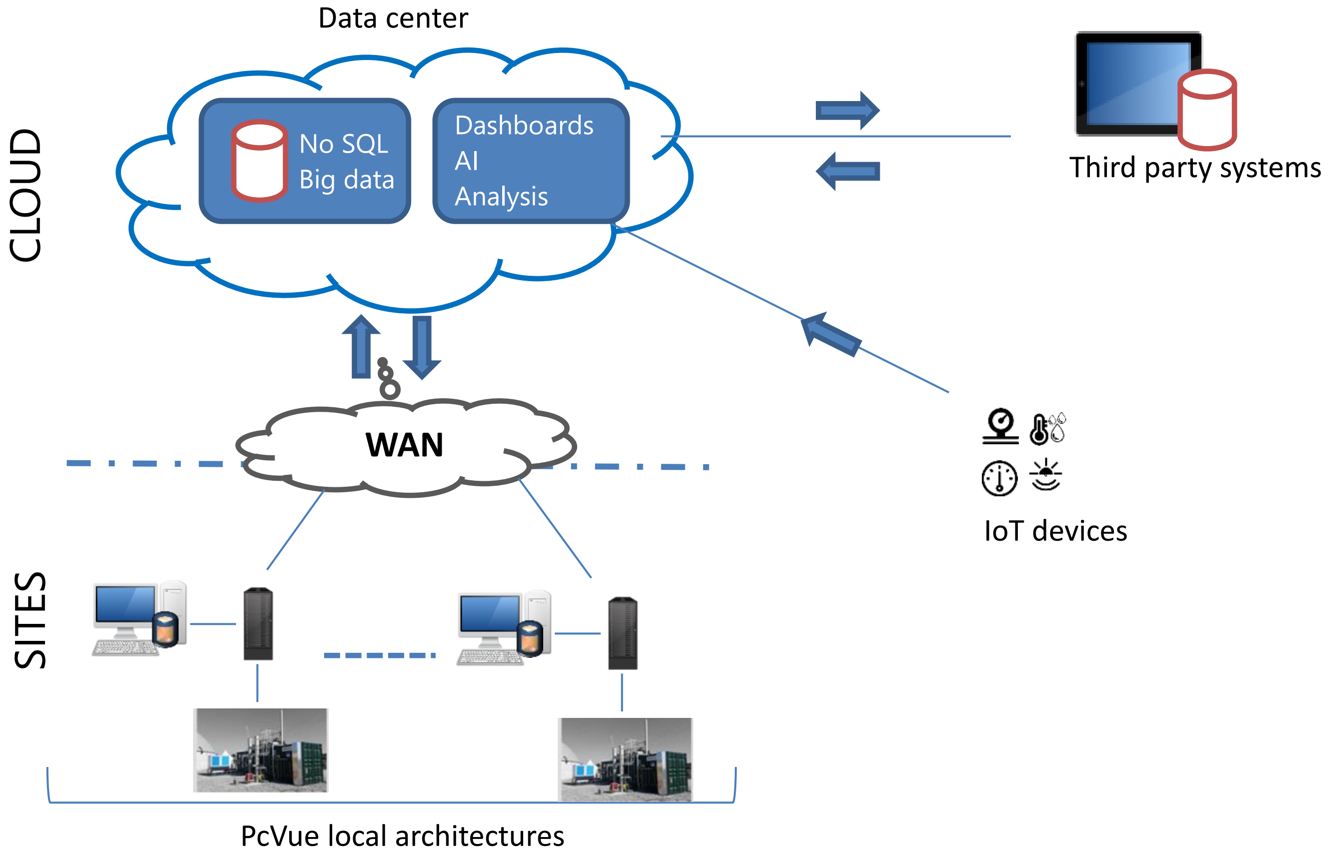


Figure 11 - Cloud Database architecture

In this architecture one or several PcVue are deployed on local sites monitoring and controlling data from local equipment. Local architecture may vary from a single station to multi-station and may include a local database.

Each PcVue site can connect a cloud database using several types of connection:

- Universal Data Connector which provides a range of ADO.net connectors

=>Dedicated for sharing & getting data from Third Party systems
=>Not dedicated for high volume of data in realtime

- MQTT driver

=> For real time data exchange of high amount of data

This architecture allows PcVue to take advantage of a cloud database to:

- share any data needed for a third-party system such as an ERP, another SCADA, or others
- get data from any IoT devices which are not part of the local architecture

2.7.2 Architecture #2: Cloud hypervision

- ✓ Delegation of infrastructure and data control
- ✓ Resources scalability
- ✓ Deploy Web & mobile clients to access any data

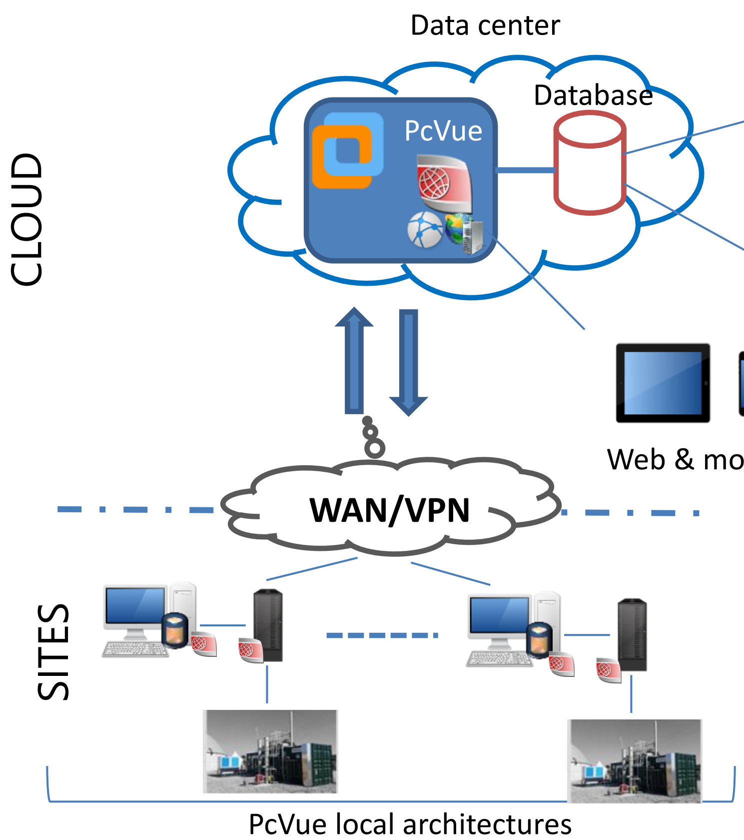


Figure 12 : Cloud hypervision

At the site level, one or several PcVue are deployed monitoring and controlling data from local equipment. Local architecture may vary from a single station to multi-station and may include a local database.

At the cloud level, PcVue is hosted in a virtual machine. A multi stations architecture may be used with several VM if needed.

It gathers data from local PcVue sites through a secured WAN network using TCP/IP multi-station messaging or other drivers.
Web and mobile clients can be deployed from the VM.

Data from third party systems as well as IoT devices can be gathered from a database using the universal data connector or MQTT.

This architecture allows to :

- ✓ Delegate the management and maintenance of the infrastructure and data to a third-party
- ✓ A high resources scalability with a minimum effort
- ✓ Deploy Web & mobile clients to access any data

2.7.3 Architecture #3: Hybrid Cloud

- ✓ Cloud data hosting
  - o Maintenance
  - o Security
- ✓ Hypervision from a physical control center
- ✓ Integration into an existing infrastructure

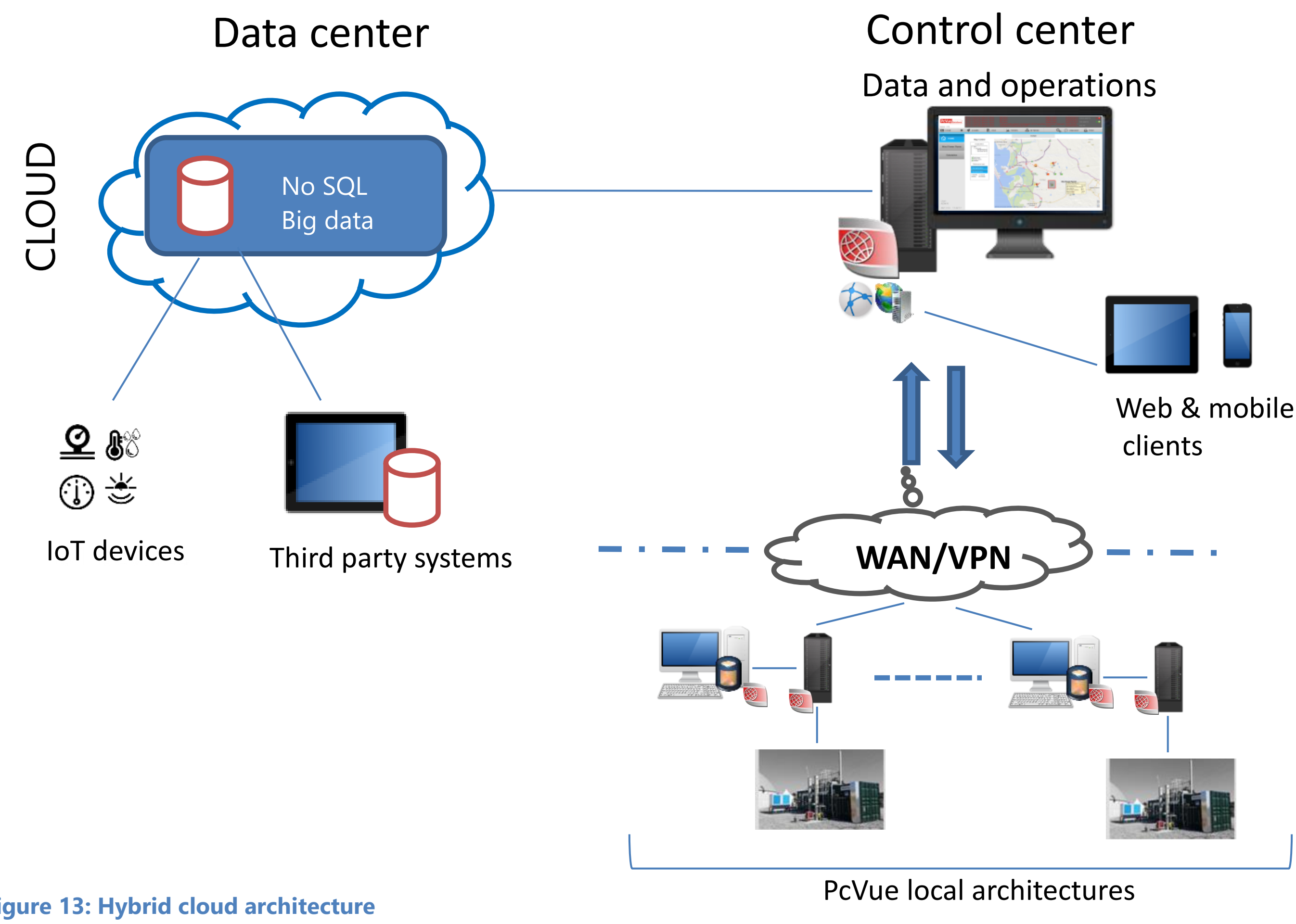


Figure 13: Hybrid cloud architecture

In this architecture PcVue is hosted on premises in a control center within an architecture which may includes sevral data acquisition servers and clients.
Data are hosted in a cloud database. PcVue gets data from third party systems or IoT devices connected to the database using UDC or MQTT. It may also records data into the database.
PcVue gathers data from local PcVue sites through a secured WAN/VPN network using TCP/IP messaging or others drivers and acts as a server for web and mobile clients.

This architecture allows to :

- ✓ Hosts data in the cloud and delegate the maintenance and the security of the data
- ✓ Integrate a cloud infrastructure into an existing architecture

2.8 Engineering station with version management

- ✓ Easy maintenance and deployment of a project and/or libraries
- ✓ Unlimited number of versions
- ✓ Modifications tracking
- ✓ Reduce the risk of errors and loss

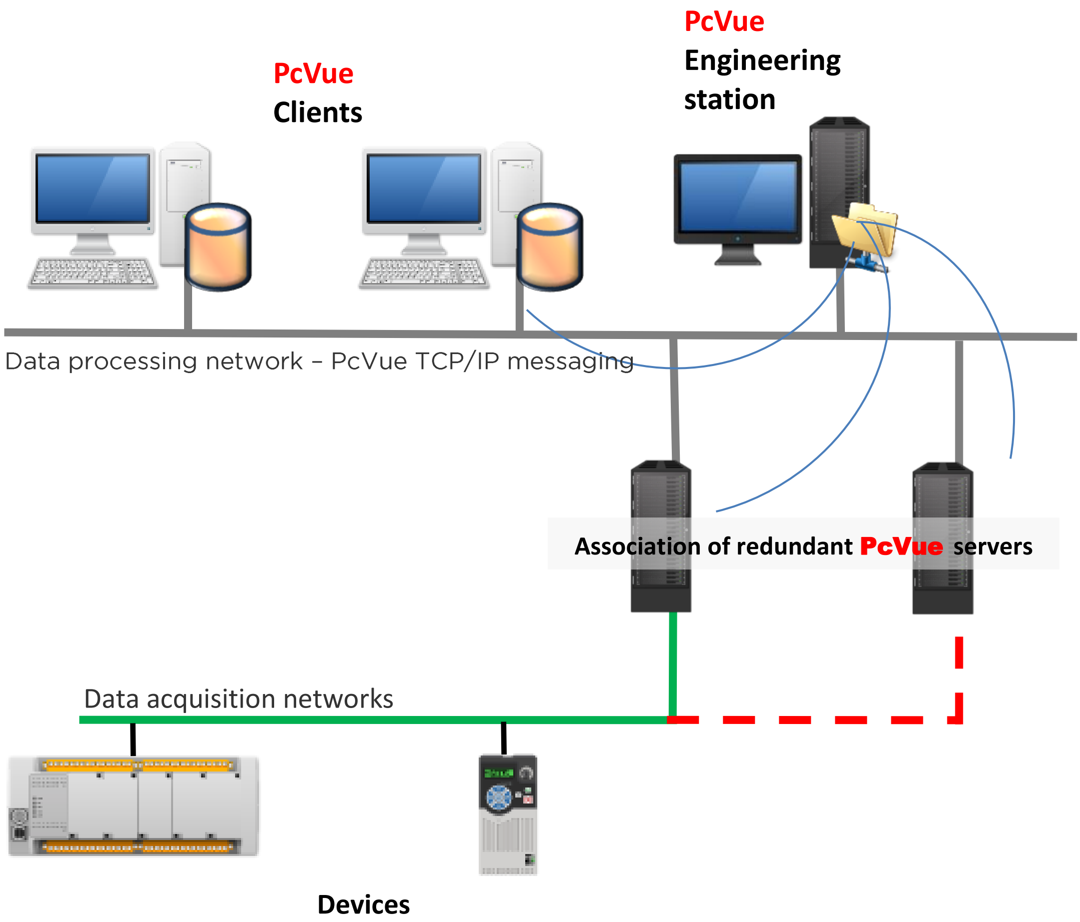


Figure 14 - Engineering station

To make the maintenance and the deployment of a project easier and faster, PcVue is delivered with a **built-in central project management tool**.
Different versions of a project and/or libraries are centralized in a shared directory on the network. They can be loaded and modified from any station on the network.
Usually a dedicated PcVue engineering station is used to host the central versions directory and to make the change for a project.

Any station can load and run manually any type of version, or automatically one reference version of a project and/or libraries from the central project directory.
The features supported are:

- 3 types of versions : development, operational and reference
- Configurable content of a version
- Track modification for each version
- Automatic version numbering system
- Unlimited number of versions (vs media free space)

2.9 Web and mobile architectures

This section describes best practices and common patterns for deploying web-and-mobile-ready architectures for PcVue 12 and above.

PcVue 12 comes with several improvements regarding the deployment of web and mobile components and integration into IT environments at large.
In particular, it is possible to separate the web server layer from the Industrial Network.
It is highly recommended to take advantage of this new separation of duties capability and to have a Web Server machine isolated from the Industrial or SCADA network on a DMZ.

However, this may not be practical in all deployment scenarios, in particular in smaller-scale systems, which is why this document puts a focus on various different deployment scenarios:

- Simplified approach for standalone all-in-one setups,
- Large scale enterprise SCADA/HMI systems,
- Remote access to small-scale systems

2.9.1 EasyMobileTechnology

Web and mobile solutions of PcVue lean on a proprietary exclusive technology EasyMobileTechnology allowing to setup mobile architecture with no gateway/plug-in, embedding all the necessary security features (https, Oauth, certificates) and the HTML5 technology as well as maintenance tools.

This technology fits the following criteria:

- No gateway, no extra plugin
- No installation on client side
- Easy settings – no scripts – Wizard only

- Open to third-party application
- Adapted to any users: end-user, SI, IT
- Secure scalable architectures and communication
- Easy Diagnostic

2.9.2 Web deployment console

The web deployment console is a component for setting, deploying and maintaining a web or mobile architecture.
It supports the following features:
- ✓ Deployment of web services and web apps on IIS
- ✓ PcVue Web Back-end endpoint management
- ✓ Data protection management
- ✓ Certificate management
- ✓ User access logging & OAuth Server management
- ✓ IIS auditing / diagnosis

The web deployment console runs on a server hosting a web server IIS.

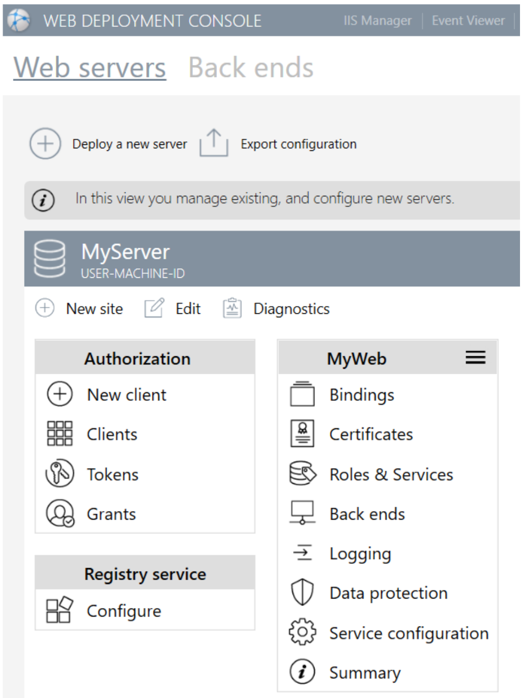


Figure 15 – Web deployment console interface

2.9.3 Web & mobile client

2.9.3.1 HTML5 Web clients

WebVue is a web client using a web browser and an internet or intranet connection to provide remote display and control of PcVue project. A user with appropriate user rights (user name and password) is able to access the PcVue SCADA application from anywhere on the network. WebVue is independent of the operating system as it runs in a web browser and it displays PcVue mimics directly without requiring any modification.
Communication between the PcVue Web Server and the WebVue client uses Microsoft IIS technology and the enterprise firewall jointly to manage security.

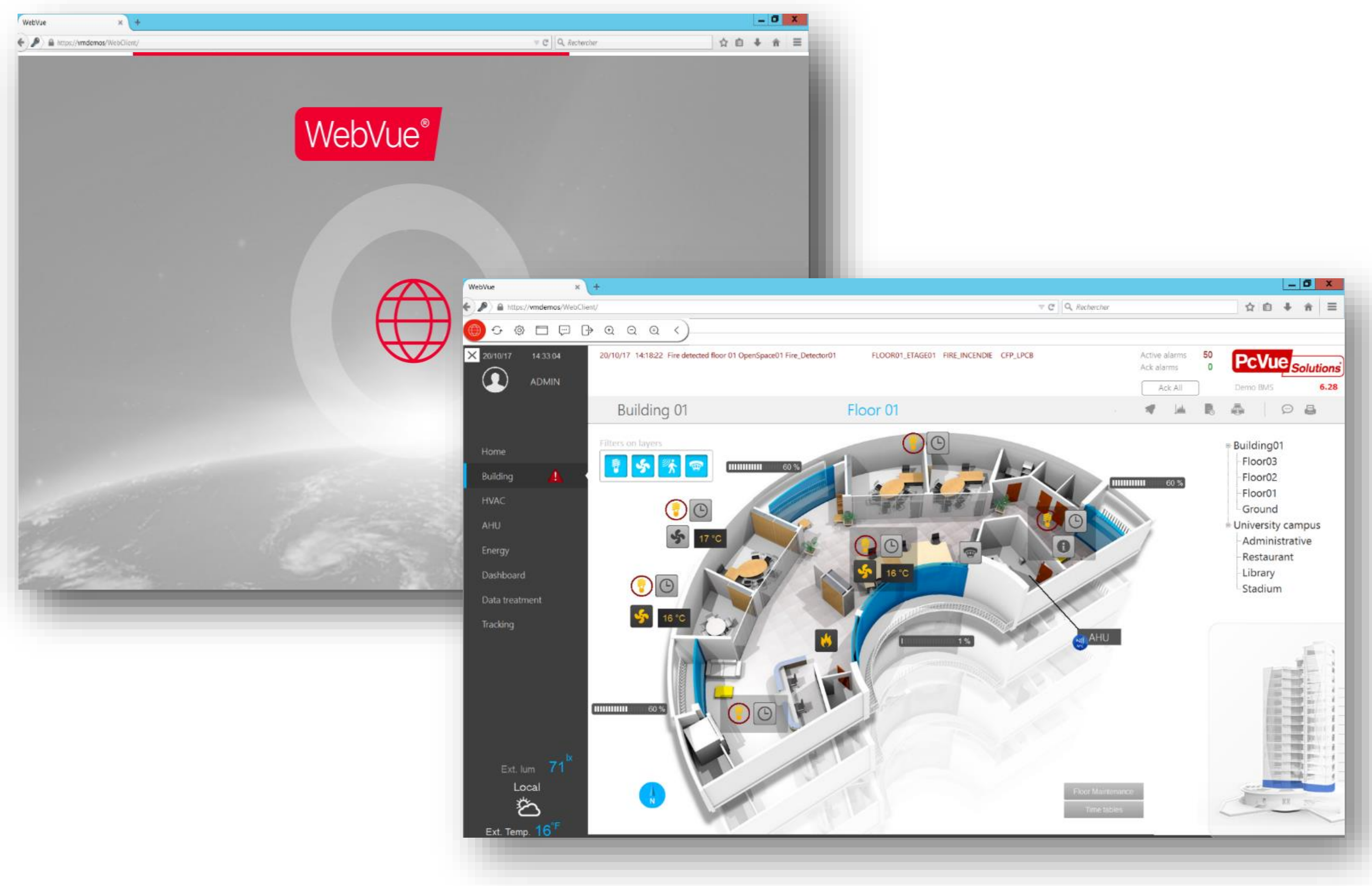


Figure 16 - HTML5 web client screenshots

2.9.3.2 TouchVue - Mobile application with alarms & events notification services

The TouchVue mobile application allows mobile devices (tablets, smartphones ...) to access the PcVue Web server public Web services with real-time values of variables and different alarm and history lists as well as curves trends. The operator can thus acknowledge an alarm or force a setpoint for example.

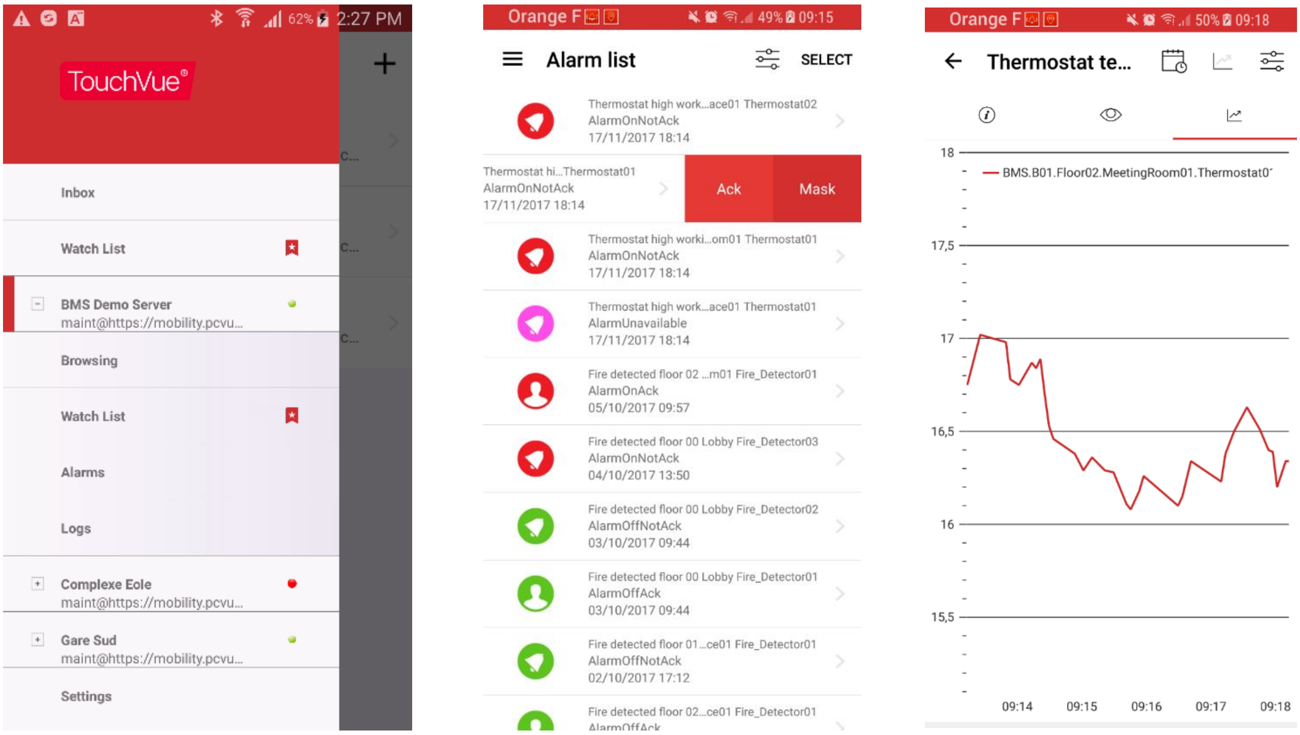


Figure 17 - TouchVue client screenshots

2.9.3.3 SnapVue – Mobile Application mobile based on location

SnapVue is a mobile application which, associated with the contextual server of a PcVue project, allows the mobile user to access, without having to navigate, the information that concerns them according to their location and role. They are then able to view and/or control the equipment that surrounds them through an interface that can be customized during the design phase.
Different services facilitate operation, such as a messaging system to exchange messages (voice, videos, texts, images) with other users and/or with the PcVue server. A bot system can also assist the user by responding to predefined scenarios.

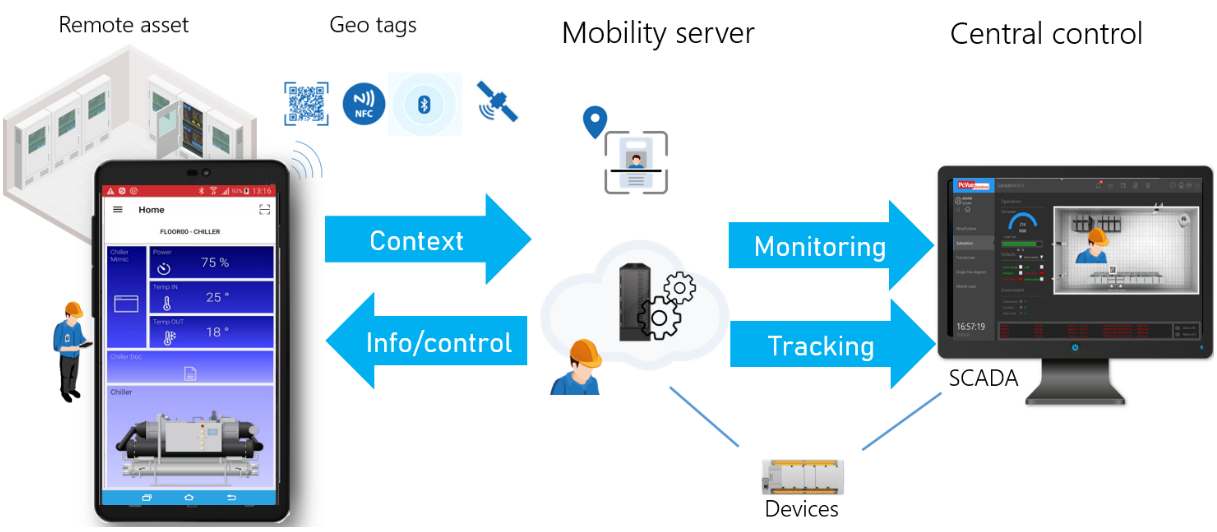


Figure 18 – SnapVue : concept

SnapVue uses geolocation technologies and services as shown below:

Figure 19 – SnapVue : technologies

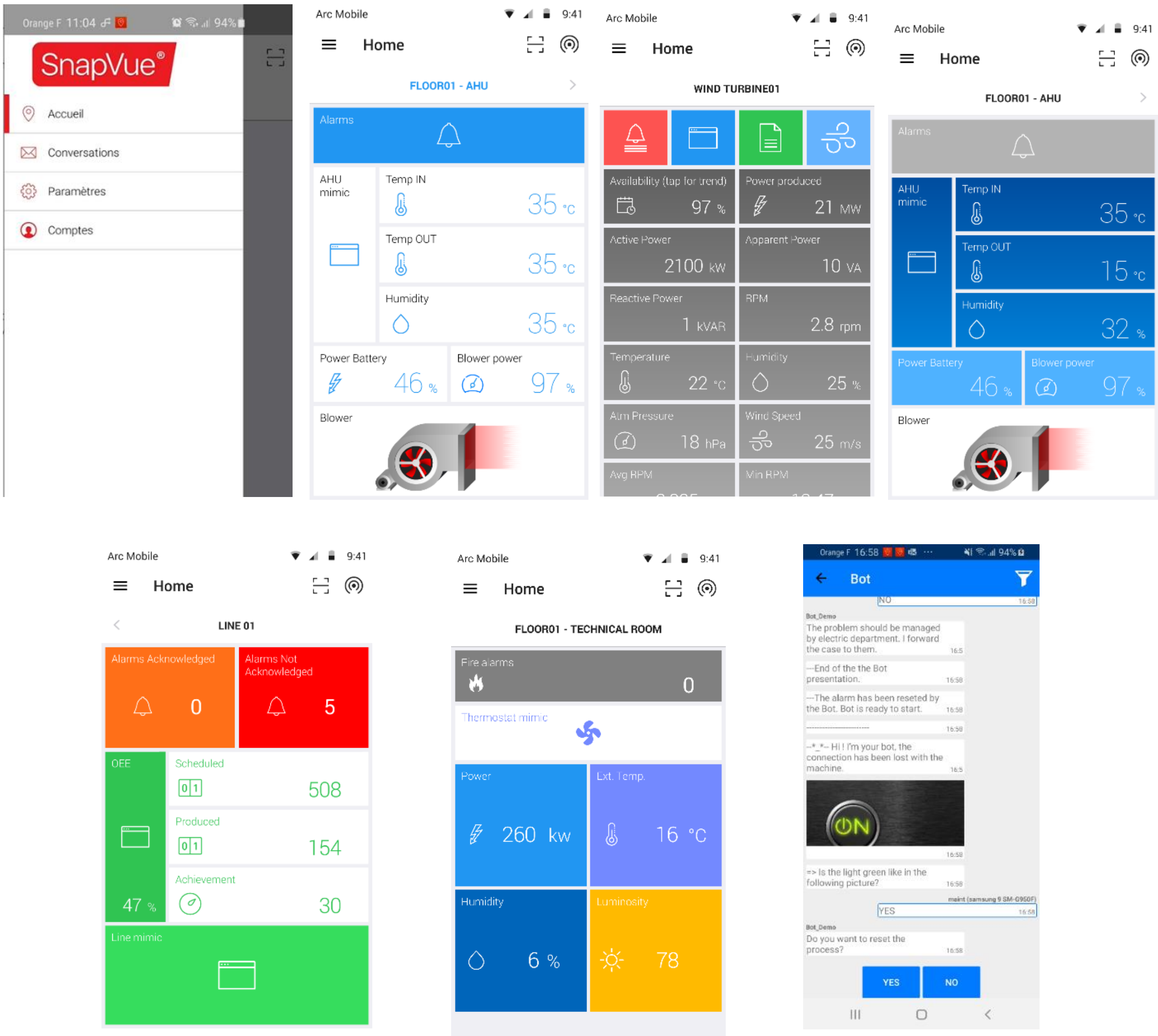


Figure 20 – SnapVue : screenshots

2.9.4 Remote Desktop Access

PcVue can be run remotely using Windows Remote Desktop feature from a PC or other terminal.
HTML5 technology will also make it possible to take advantage of this functionality from any internet browser.

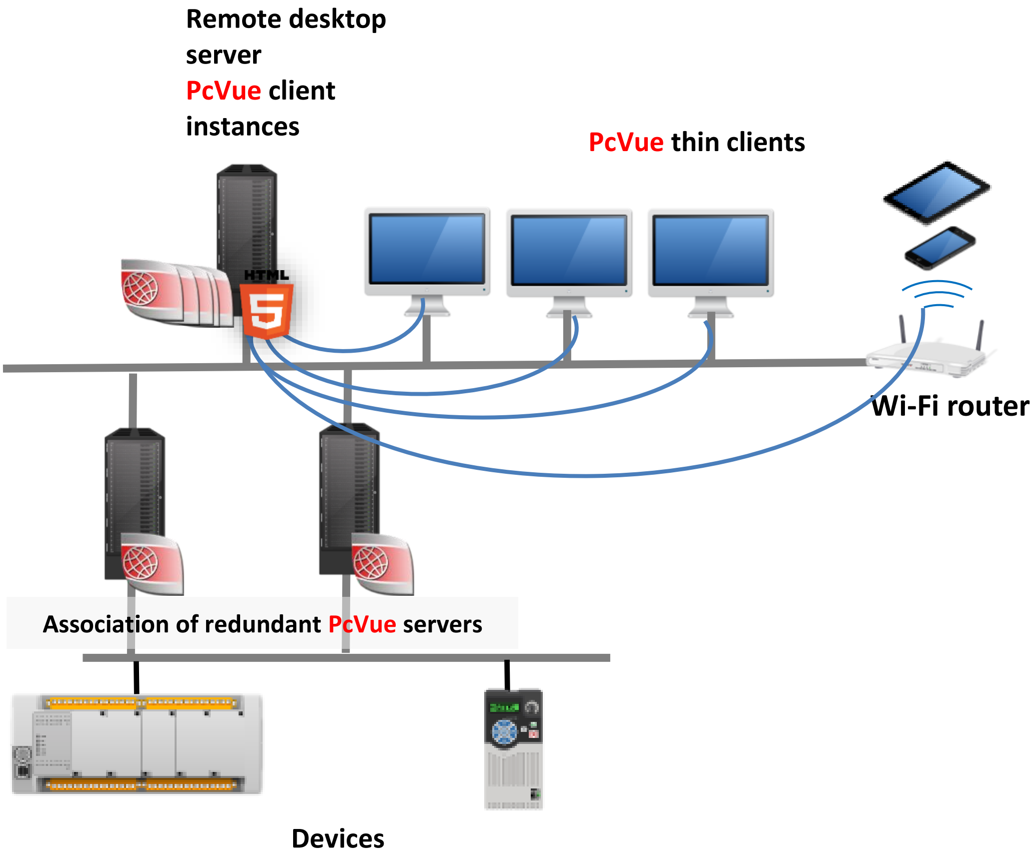


Figure 21 – Remote desktop access

2.9.5 Architecture #1: All-in-One Deployment

- ✓ Simplified approach for standalone all-in-one setups
- ✓ Low level of security
- ✓ Intended when the network is private and fully isolated from outside access

2.9.5.1 Description

In this deployment scenario, the PcVue Web back end station and the Web Server Components are not separated. They are hosted and run on the same computer.

The Web & Mobile Clients including WebVue and TouchVue are connected to the same network as the Web Server.

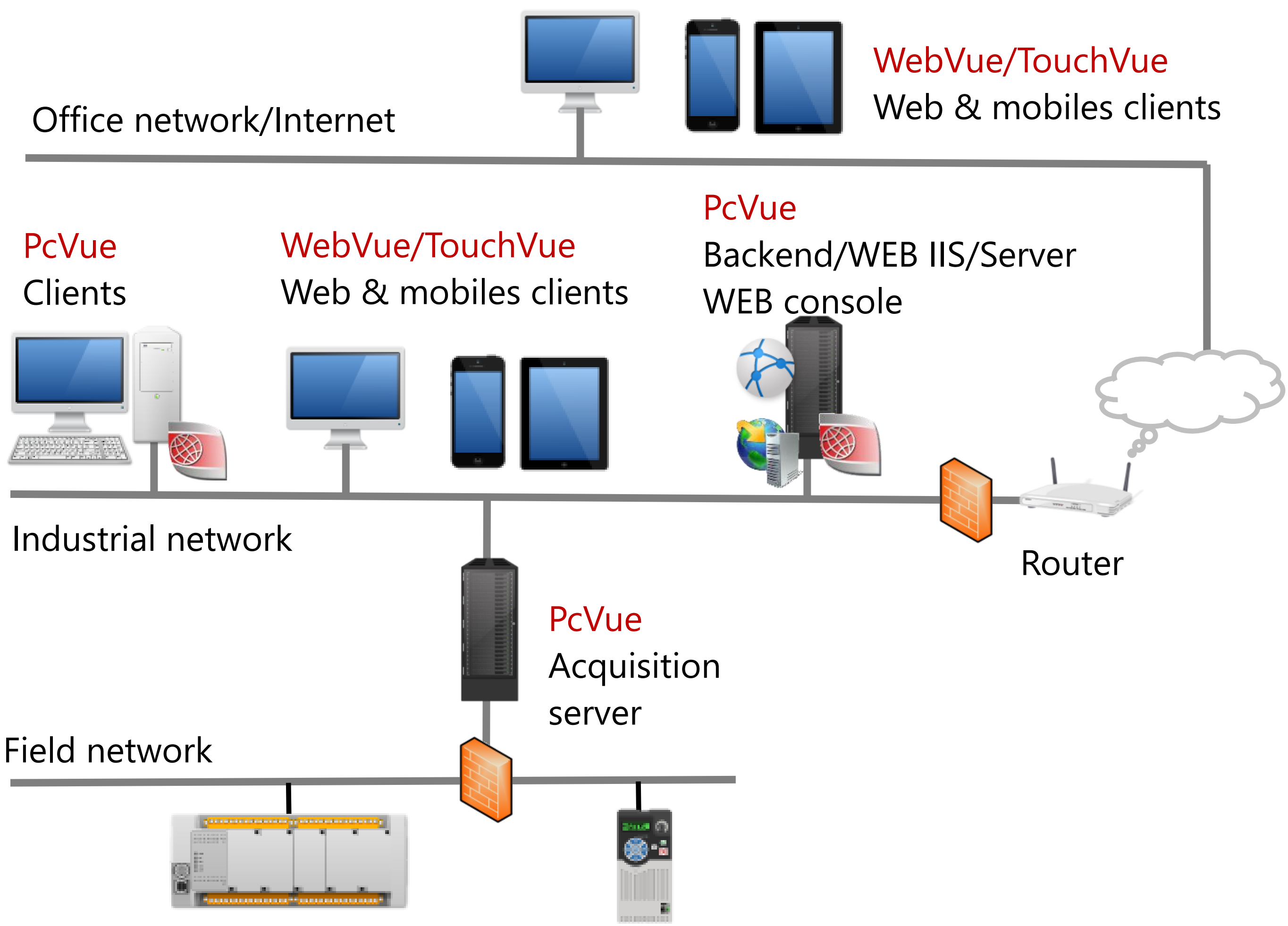


Figure 22 – Architecture #1 – All-in-one deployment

Note:

- IP ranges and addresses are purely illustrative according to typical usage patterns as described in RFC 6890. Any other subnets range or set of addresses may be used as well.
- The architecture of the PcVue SCADA system is purely illustrative and may differ from your actual setup.
- The separation of the industrial network from the automation network, although recommended, is purely illustrative.

2.9.5.2 When to use?

This architecture is intended for deployment scenarios when Web & Mobile clients are on the same subnet as the PcVue Web back end station.

Usage of this deployment scenario is considerable when the network (the subnet) is private and fully isolated from outside access. In particular, computers and devices used by operators shall not have access to the outside world neither, to avoid the risk of being used as a door to the Industrial Network.

2.9.5.3 When not to use?

Do not use this deployment strategy when the network is open to incoming requests from outside networks or open to unprotected access from unknown devices.

In particular, do not use this deployment strategy when access from web and mobile client systems on the Internet is required and no further means of network security (such as VPN-tunneling for instance) are available.

2.9.5.4 Requirements

1. The deployment of this architecture requires a minimum level of network expertise.

2. Requires all computers and mobile devices to be on the same subnet, typically the Industrial network, including Web & Mobile clients, the Web Server and the PcVue Web back end station.

3. Clients on this network are supposed to trust the Web Server machine without reservation, as they are on the same and, by definition, private network.

4. This architecture works with minimum requirements towards the trustworthiness of the web server certificate.
   A certificate from a certificate authority is not mandatory to establish trust with the Web Server.

2.9.5.5 Benefits

1. Only a single computer is necessary to host both the PcVue Web back end and the Web Server.

2. This computer does not require more than one network interface card.

3. Works out of the box when using the IP address of the Web Server computer to connect web & mobile clients.

   A DNS is not required for name resolution on Windows platforms. The Web Server computer may be addressed by its hostname from any Windows-based web clients.

   Can work with a Windows desktop operating system such as Windows 10 on the PcVue Web Server computer if serving a limited number of users. In all cases, the usage of a server operating system is highly recommended.
   When using non-Windows client devices (Android, iOS, Linux), the presence of a DNS server is a must for name resolution. This can be achieved by using a Windows Server operating system for the PcVue Web back end station and the activation of the DNS server role.

4. Usage of a self-signed certificate works out-of-box, with the need to add a security exception on the web client's user agent or to enable the option "Ignore Certificate Errors" on mobile client applications.

   If there is an Active Directory server accessible from the network, a domain certificate may be issued from the Active Directory server and trusted by all the clients of the domain (by domain policy or via a corporate MDM system).

2.9.5.6 Limitations

1. Expect limitations when hosting the Web Server on a Windows desktop operating system. In particular the maximum number of client connections IIS can handle is limited.

2. Microsoft® Edge does not allow storing cookies if the hostname is not a FQDN. This causes troubles with web components. It can be overcome by changing the URL to:

```
https://<hostname>.local
```

3. Limited performance may be experienced, particularly during WebVue client loading, when using invalid (partly trusted or untrusted) certificates because in such circumstances, files are not cached by web browsers.

2.9.5.7 Web Deployment Console

This architecture can be easily deployed using the “Quick Setup” wizard of the WDC with all settings left to their default value.
Therefore, the WDC needs to be installed on the same computer as the PcVue Web back end and the Web Server.

2.9.6 Architecture #2: Network isolation and DMZ

- ✓ Large scale enterprise SCADA/HMI systems
- ✓ High level of security
- ✓ Intended when the web/mobile clients are outside the industrial network

2.9.6.1 Description

In this deployment scenario, the PcVue Web back end station and the Web & Mobile clients are on different physical or logical networks, in different security perimeters, requiring segregation with a DMZ. The inner network (LAN side of the DMZ router) is a private secure network. The outer network (WAN side of the DMZ router) is a less trusted network, typically a corporate office network or the Internet.

The Web Server Components are hosted on a computer inside the DMZ and the PcVue back end is hosted on the secure network.

This architecture provides the best integration into IT networks and allows for maximum compliance with IT guidelines and practices.

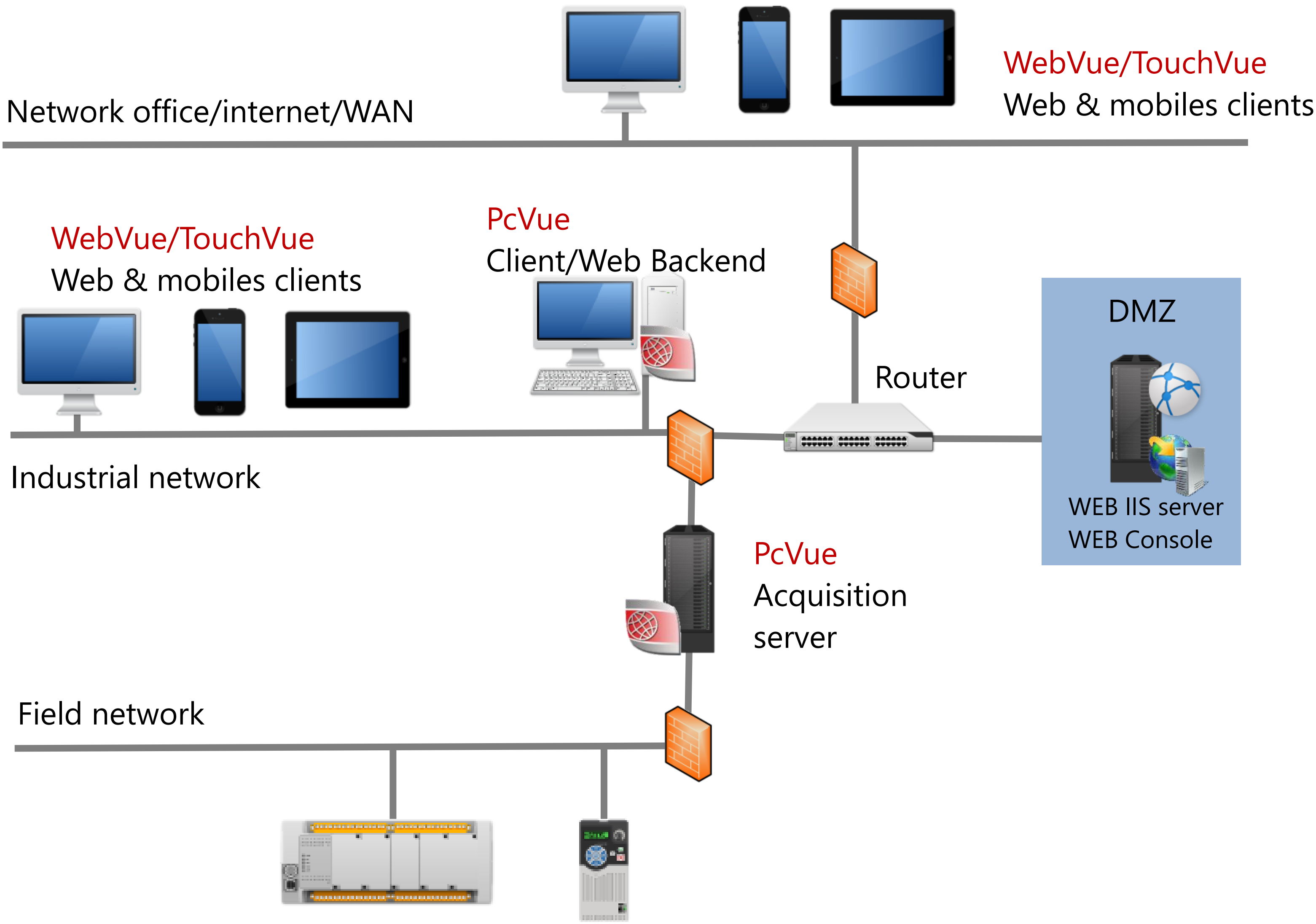


Figure 23 – Architecture #2 – Network isolation and DMZ

Note:

- IP ranges and addresses are purely illustrative according to typical usage patterns as described in RFC 6890. Any other subnets range or set of addresses may be used as well.
- The architecture of the PcVue SCADA system is purely illustrative and may differ from your actual setup.
- The separation of the industrial network from the automation network, although recommended, is purely illustrative.

2.9.6.2 When to use?

Usage of this deployment architecture is recommended whenever the Web & Mobile clients are not on the secure industrial network.

2.9.6.3 Requirements

1. The level of network and IT expertise required to deploy this architecture is intermediate to high.

2. Requires a suitable network infrastructure to segregate the private network from the lesser protected network. This includes a router (and adequate configuration of routes) and at least one firewall.

   Common DMZ architectures are supported, including single firewall setup and dual firewall setup:

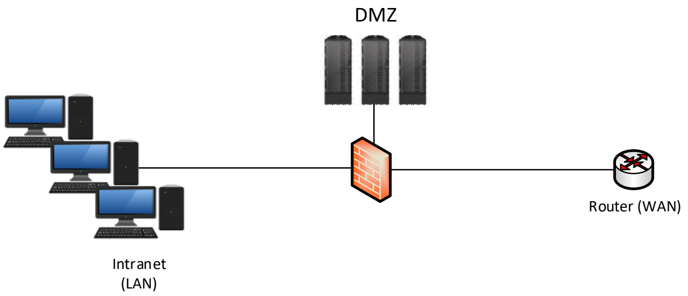


Figure 24 - DMZ – Single firewall setup

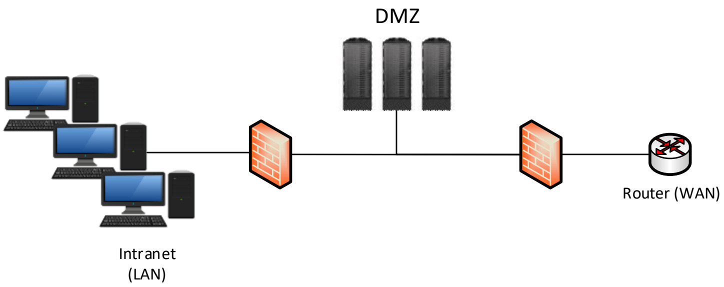


Figure 25 - DMZ – Dual firewall setup

3. Support of the end user's IT department is likely to be required to properly set up network segregation, name resolution and certificates.

   This includes the proper configuration of:
   - DNS

- Routing
- Network Address Translation (or Port Forwarding)
- Certificates

An Active Directory infrastructure is likely to be required as the corporate PKI for issuing certificates and to ensure trust relationships as part of a global policy.

4. In order to validate the identity of the Web Server computer on the lesser trusted network and to prevent Man-in-the-Middle attacks, usage of a fully trusted certificate is a must.

   - This certificate can be issued by the IT department (corporate network Active Directory server). It is enough if all web & mobile clients are in a trusted relationship with the corporate network infrastructure.

   - This certificate can be issued by the IT department via a trusted CA. Necessary if the Web Server is accessed by external Web & Mobile clients (typical access from the Internet by client devices/computers not in a trusted relationship with the corporate network infrastructure).

   - This certificate may be issued via the Let's Encrypt® wizard of the WDC if an Internet access exists and if the user organization policy allows the Let's Encrypt® service.

5. A DNS server able to resolve the Web Server name is required on the lesser trusted network.

6. A Windows Server operating system on the Web Server computer, and ideally also on the PcVue Web back end station.
7. The PcVue Web back end station must be accessible from the Web Server computer at least by its IP address. Access via hostname is also possible, given that a mean of name resolution is present from within the DMZ:
   - A dedicated entry in the *hosts* file of the Web Server computer.
   - A DNS server within the Industrial network that is accessible from the DMZ. If not already available, the activation of the DNS-Server role on the Windows Server operating system of the PcVue Web back end station can be a solution.

   Note: Allowing access from a computer within a DMZ into the private network contradicts with DMZ common patterns and practices. For technical reason however, TCP port 8090 needs to be opened into that direction.

2.9.6.4 Benefits

1. This architecture allows for convenient access from less trusted networks, typically the Internet or Intranet, by exposing the web and mobile services and applications of the Web Server under a Fully Qualified Domain Name.
2. It allows maximum control over network traffic, in line with IT network segregation practices, making sure that there are no undesirable incoming connection requests from outside networks into the industrial network, including traffic control and monitoring at network perimeters.

2.9.6.5 Web Deployment Console

This architecture can be deployed by using any of the WDC setup wizards. The default settings of the “Quick setup” wizard will not be suitable in all situations. The WDC needs to be installed on the Web Server computer.

2.9.7 Architecture #3: Simplified NAT scenario for remote access

- ✓ Remote access to small-scale systems
- ✓ Intended when no managed IT infrastructure is available.

2.9.7.1 Description

This deployment scenario corresponds to a single private LAN, the Industrial network, where both the Web Server, the PcVue Web back end station and most Web & Mobile clients reside. A dedicated Internet access is used for remote connections.
In this deployment scenario the Web & Mobile clients are distributed across both sides of a NAT boundary (local and remote web clients).

Although it is technically feasible to deploy this architecture as is, it is not recommended to do so without the deployment of further security measures.

The list of potential measure includes usage of a VPN and client address locking, in which case the architecture may be logically equal to Architecture #1. By using the network perimeter's dedicated DMZ port for establishing a dedicated network segment, in which case the architecture is a simplified version of Architecture #2. In any case, it is recommended to separate the PcVue Web back end station and the Web Server as described in Architecture #2, which by itself is an additional security measure.
If the Internet access is provided via a 3rd party and requires a device such as a set-top-box supplied and operated by the ISP, it is strongly recommended to install an appliance designed to control the network perimeter. In particular, it is recommended to refrain from alternative solutions, such as the "Exposed Host" pattern.

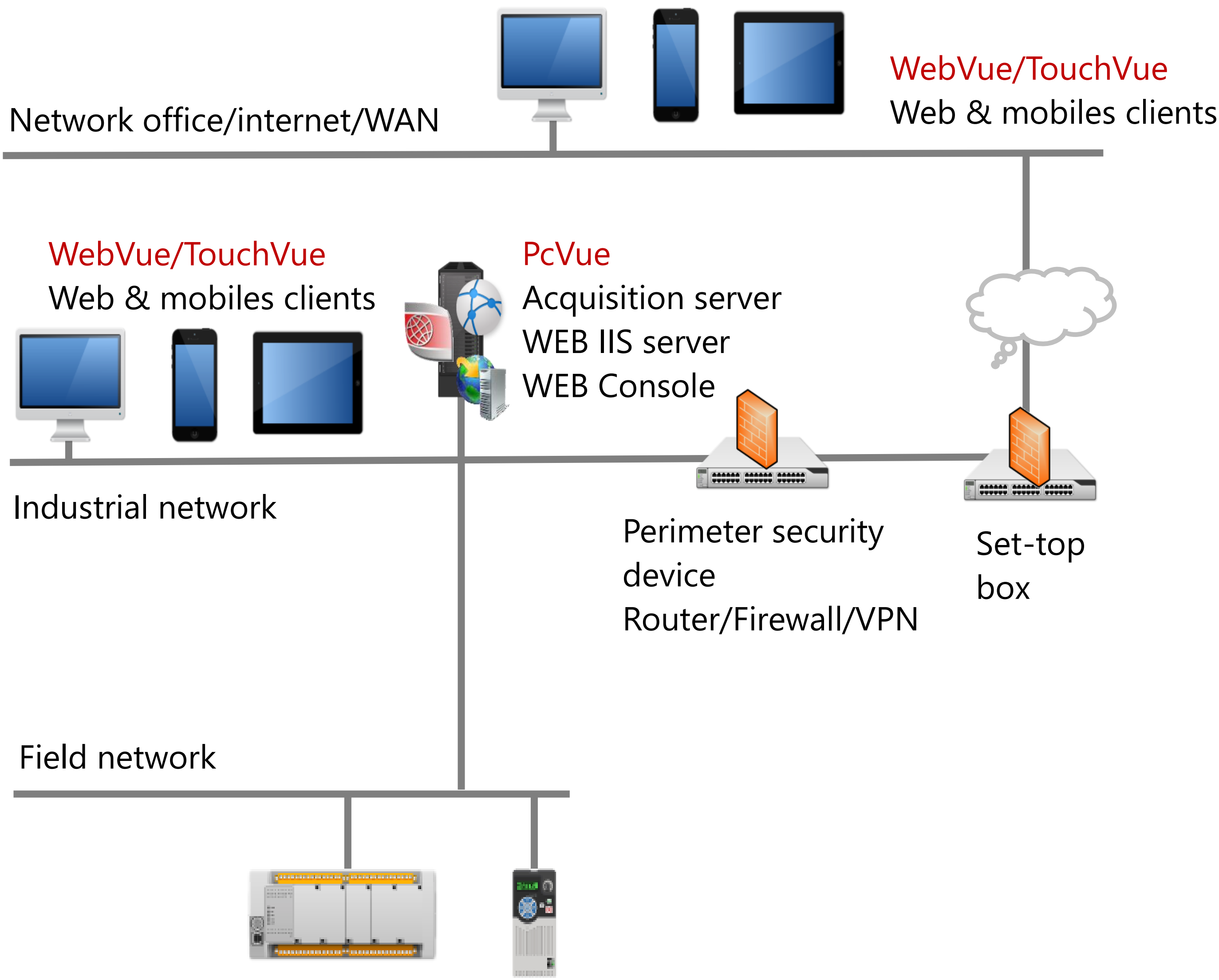


Figure 26 - Architecture #3 – Simplified NAT scenario for remote access

Note:

- IP ranges and addresses are purely illustrative according to typical usage patterns as described in RFC 6890. Any other subnets range or set of addresses may be used as well.
- The architecture of the PcVue SCADA system is purely illustrative and may differ from your actual setup.
- The IP address under which the router device is exposed to the WAN may depend on your ISP.

2.9.7.2 When to use?

This deployment scenario may be required for simple remote access when no managed IT infrastructure is available.

We recommend that existing systems using this type of architecture to run legacy WebVue versions are migrated to Architecture #2 or to apply additional security measures.

2.9.7.3 When not to use?

Do not use this architecture as is in production environments or real-life system without understanding the risks associated to poor network segregation and weak network traffic control.

2.9.7.4 Requirements

1. The level of network and IT expertise required to deploy this architecture is low to intermediate.

2. The network infrastructure to make a connection between the private network and the lesser protected network. The network infrastructure to connect the Web/Mobile Clients on either side of the router.

3. Network Address Translation (or Port Forwarding specifically) configured on the network boundary.

4. In order to validate the identity of the Web Server computer on the lesser trusted network and to prevent Man-in-the-Middle attacks, usage of a fully trusted certificate is a must.

   - This certificate can be issued by the IT department via a trusted CA. Necessary if the Web Server is accessed by external Web & Mobile clients (typical access from the Internet by client devices/computers not in a trusted relationship with the corporate network infrastructure).

   - This certificate may be issued via Let's Encrypt® wizard of the WDC if an Internet access exists and if the user organization policy allows the Let'Encrypt® service.

5. The Web Server computer must be accessible by the Web & Mobile clients from both network segments.

This can be achieved if the Web Server is well-known on both network segments under the same FQDN.

If this is not the case the possibility for the Web & Mobile clients to directly connect to the Web Server computer by using its FQDN without the messaging having to leave the private network is required. Usage of NAT Loopback / Hairpinning is suggested in this case.

If none of these options is possible, it is recommended to create two different sites via the WDC, which both connect to the same PcVue Web back end station.

2.9.7.5 Benefits

1. This architecture allows for convenient access for Web & Mobile clients located on the Industrial network and from the Internet.

2. This architecture is a first step in a migration process of legacy WebVue systems offering remote web access.

2.9.7.6 Limitations

This deployment scenario offers limited network security if a specific appliance is not added to control the network perimeter, since:

- You rely on a set-top-box owned by an ISP to control the network perimeter and remote connection,
- And as a consequence, a computer that is part of the Industrial Control System should be considered directly exposed to the Internet.

In a worst-case scenario potential security vulnerabilities on several levels could be exploited by an attacker to gain access to the Industrial Control System.

2.9.7.7 Web Deployment Console

This architecture can be deployed by using any of the WDC setup wizards.
The WDC needs to be installed on the Web Server computer.

2.10 Full architecture

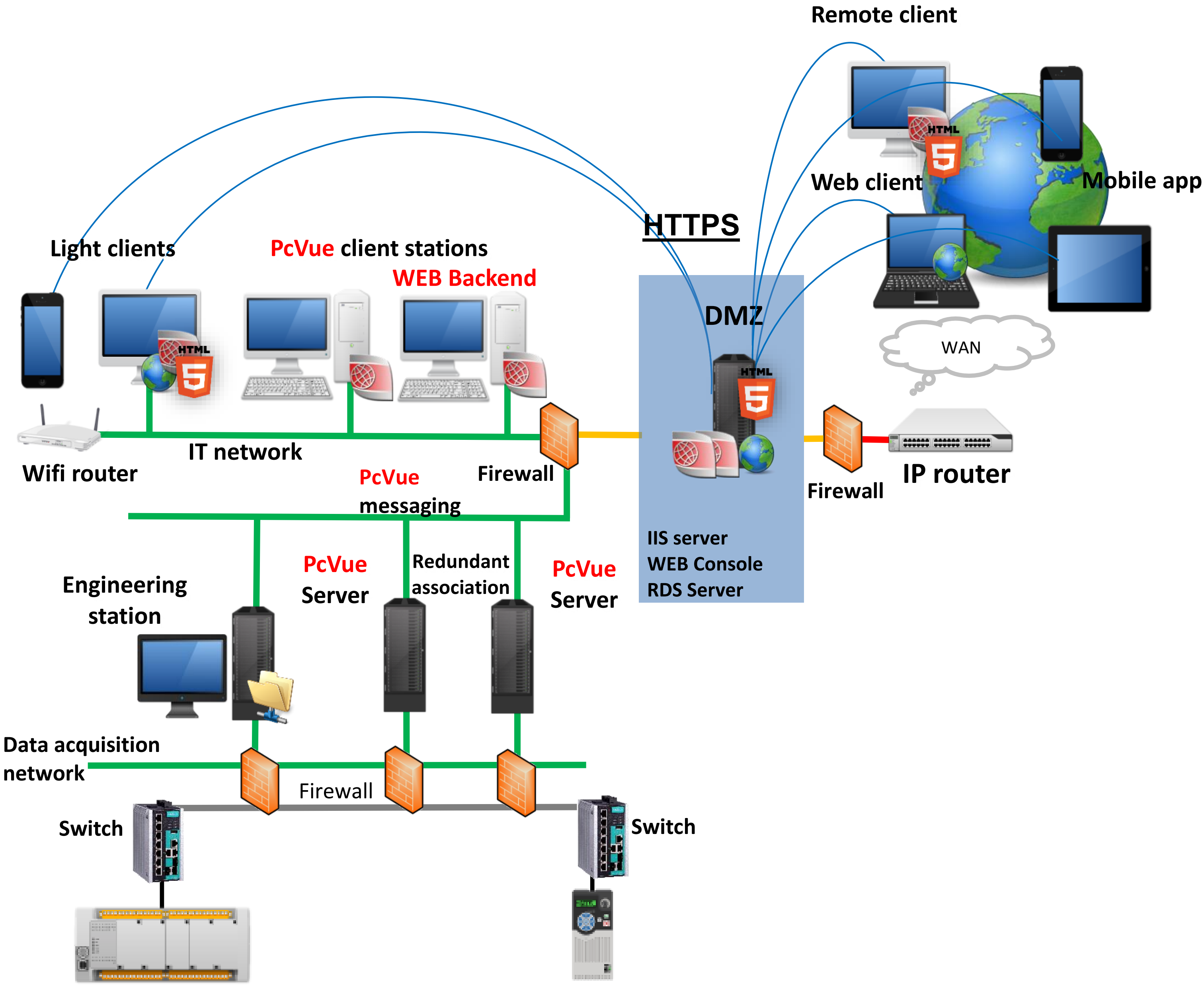


Figure 27 - Full architecture

This example of architecture leans on the following elements:

- The data acquisition is performed by redundant acquisition servers on the industrial network.
- A development station is used for the centralized management of the project.
- The operation is performed by the client's stations on the computer network isolated by a firewall

- One client station acts as a web backend
- A station installed on a Windows server in a demilitarized zone (DMZ[1]) isolated by firewalls, hosts a web server, a mobile server and a Windows RDS[2] Server.
- Clients can be run remotely through RDS instances using the Windows Remote Access Office.
- An interface installed on the server allows the display of client instances on any device that supports HTML5.
- The web clients allow operation from a standard web browser.
- A mobile application connected to mobile server is used for the notification and acknowledgment of alarms and control from a smartphone or tablet.
- The exchanges between the Web server and terminal use secure sockets HTTPS[3].
- Users access of the entire system is managed by Windows Active Directory for single sign-on (SSO[4])

A number of precautions must be taken to protect the components of a PcVue multi-level architecture.

Thus, the necessity to:

- Segment the various networks (computer and industrial for example) by the creation of separate logical areas (VLAN[5]) that require the same level of security

- Filter the data by using firewall.

The use of a DMZ and routers also allows to isolate the network from the outside and prevent unwanted intrusions.

The establishment of VPN[6] tunneling solutions may also be necessary to protect traffic between two network components. Typically, a VPN can be established between a PcVue acquisition station and a PLC communicating via TCP / IP, or

[1] Demilitarized Zone
[2] Remote Desktop services
[3] HTTPS : HyperText Transfer Protocol Secure
[4] Single Sign-On
[5] VLAN : Virtual LAN
[6] VPN : Virtual Private Network

between multiple remote monitoring sites communicating with inter-station TCP / IP messaging.

PcVue Solutions, in partnership with MOXA offers a complete solution of hardware protection to address the issues mentioned above:

- Full range of secured Firewall / VPN industrial
- Traffic limitation and control between different network zones
- Creation of traffic restrictions

2.11 Virtualization

- ✓ To reduce the number of physical stations
- ✓ To reduce the administration effort and cost
- ✓ Low-cost thin clients
- ✓ Installation free on thin clients
- ✓ Comply with IT requirements

Virtualization, in computing, refers to the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network resources.
Hardware virtualization or platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources.
In hardware virtualization, the host machine is the actual machine on which the virtualization takes place, and the guest machine is the virtual machine. The words “host” and “guest” are used to distinguish the software that runs on the physical machine from the software that runs on the virtual machine.
Virtualization of industrial applications can benefit many departments involved: IT, Engineering and operations.[7]

[7] Source : Wikipédia

2.11.1 Application virtualization

✓The host computer can run different versions of **PcVue** or **FrontVue** in isolated environments
✓Setting up a working environment for one-off operations becomes easy
✓Setting up an ancient operating system is possible
✓Runs under Windows 7, Windows 8, Windows 8.1, Windows 2008 SP2 and 2008 R2 SP1,2012 and 2012 R2 Server and VMWare

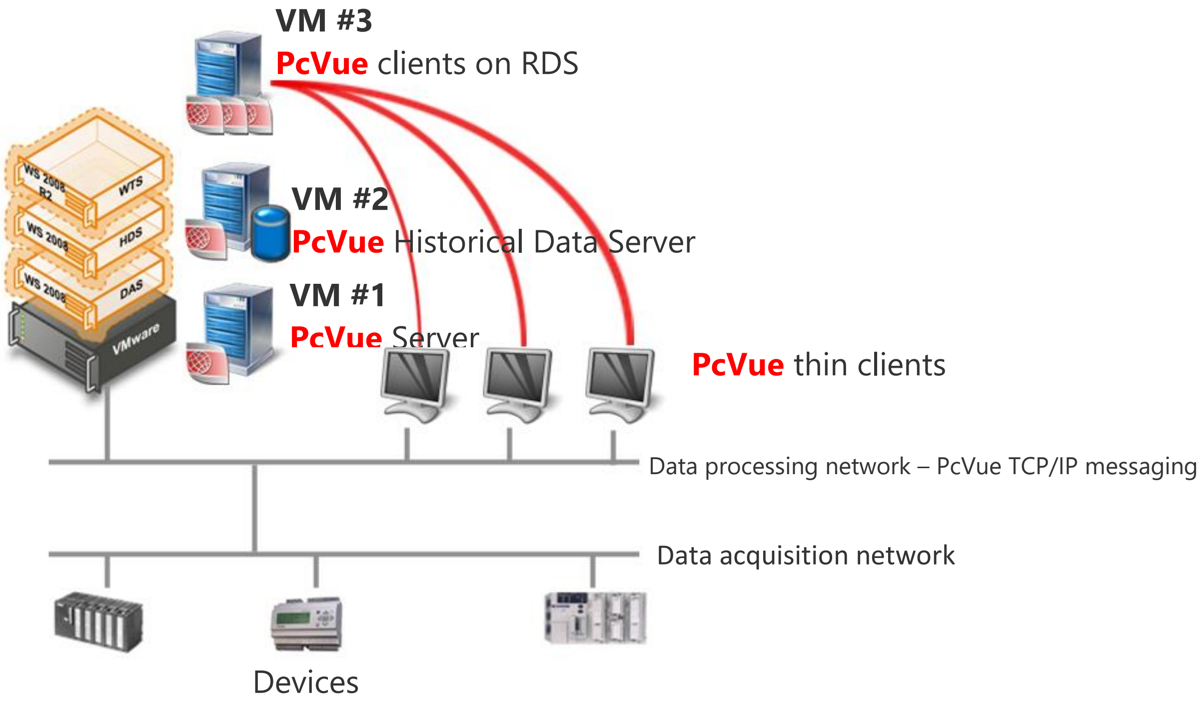
2.11.2 Resources virtualization

✓Virtualized environments can run various **PcVue** servers under different operating systems on a single physical machine

✓**PcVue** licenses can be of different types

✓Dynamic assignment of virtual machines to physical hosts according to resources optimization rules

2.11.3 Example of implementation



Here the SCADA application runs on IT administrated stations. A single physical machine with VMware or equivalent hosts all the stations in isolated Virtual Machines, one of these VM runs RDS allowing multiple RDS Client Stations to connect to the Servers. Most of the architectures described in this document can be deployed in virtual environments.

3. Glossary

Name	Abbr.	Description
Microsoft® Internet Information Services	IIS	Internet Information Services (IIS) is a web server created by Microsoft® and shipped with Windows operating systems. IIS is the built-in web server on Microsoft® Windows operating systems.
PcVue Web back end station		The PcVue station on the Industrial network used as the gateway between the PcVue multi-station system and the actual Web Server (IIS). The Web back end runs Sv32.exe, the PcVue main process.
Web Server machine Web Server computer		The computer that is running the IIS web server, which in turn is hosting the PcVue Web Server Components. The Web Server does not run Sv32.exe (PcVue main process itself).
PcVue Web Server Components		Set of services and apps installed on a Web Server machine to connect PcVue web and mobile clients.
Web & Mobile Client Systems		Computers and devices running a WebVue web client in a web browser or a native mobile app such as TouchVue, on a smart mobile device.
Web Deployment Console	WDC	The desktop application installed on the Web Server machine, which allows the system administrator to configure, deploy and monitor IIS and the PcVue Web Server Components.
Industrial Network		The network segments that includes the PcVue SCADA network. Referred to as the Level 2 Industrial network in the ANSI/ISA-95 information model (also referred to as the SCADA level).
Demilitarized Zone	DMZ	A DMZ or demilitarized zone - sometimes referred to as a perimeter network - is a physical or logical network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN).
Fullly Qualified Domain Name	FQDN	A domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including at least a second-level domain and a top-level domain.
Domain Name System	DNS	DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
Windows Internet Name Service	WINS	WINS is Microsoft®'s implementation of the NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

Name	Abbr.	Description
Subnetwork	Subnet	A subnetwork or subnet is a logical subdivision of an IP network. Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. Traffic is exchanged between subnetworks through routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between the subnets.
Virtual Private Network	VPN	A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
Firewall		It is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Network Address Translation	NAT	NAT is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. One Internet-routable IP address of a NAT gateway can be used for an entire private network.
Port Forwarding	PAT	Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.
Internet Service Provider	ISP	An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet.
Private Key Infrastructure	PKI	A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Certificate Authority	CA	A certificate authority or certification authority (CA) is an entity that issues digital certificates. The CA can be either a trusted 3rd party or part of a corporate PKI.
Mobile Device Management	MDM	Mobile device management is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on devices, enforcing corporate policies, integrating and managing mobile devices.

Name	Abbr.	Description
Hypertext Transfer Protocol Secure Hypertext Transfer Protocol	HTTP / HTTPS	The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. HTTPS (HTTP Secure) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication. The protocol is often referred to as HTTP over TLS, or HTTP over SSL.
Hairpinning		Hairpinning (also called "NAT loopback") describes a communication between two hosts behind the same NAT device using their mapped endpoint. Hairpinning is where a machine on the LAN is able to access another machine on the LAN via the external IP address of the LAN/router (with port forwarding set up on the router to direct requests to the appropriate machine on the LAN).
WebSocket(s)		WebSocket (RFC 6455) is a computer communications protocol, providing full-duplex communication channels over a single TCP connection. WebSocket is designed to work over HTTP ports 80 and 443 as well as to support HTTP proxies and intermediaries. Analog to HTTP WebSocket supports encryption through its wss-binding (Web Socket Secure).
HTTP/2 - SPDY protocol		HTTP/2 is a major revision of the HTTP network protocol. It was derived from the earlier experimental SPDY protocol. Major improvements carried by the protocol evolution concern the responsiveness of websites by introducing decreased latency, header compression, TCP multiplexing and pipelining of requests.

Some of the general-purpose definitions were taken from *Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc*. There is no guarantee of accuracy or fit-for-purpose.

Table of figures

PcVue Solutions

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

GERMANY - Munich
PcVue Gmbh

Italy - Milan
PcVue Srl

UK – London control
Technology International

USA - Boston
PcVue Inc.

Chile - Santiago
PcVue Chile

SINGAPORE - Singapore
PcVue Sea

MALAYSIA- Kuala Lumpur
PcVue Sdn Bhd

CHINA- Shangai
PcVue china

JAPAN - Nagoya
PcVue Japan

UAE - Dubaï
PcVue DMCC

swiss safety center
ISO 9001
ISO 14001
certified system

ARC Informatique
Private limited company capitalized
at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695356

PcVue Architectures & Deployment