PcVue Best Practices Guide to effectively secure your system

2024

WHITE PAPER

SECURING SUPERVISION OF INDUSTRIAL AND AUTOMATED SYSTEMS

WHO IS THIS DOCUMENT FOR ?

This document presents the questions that should be asked to secure the supervision of an industrial and automated installation, and describes good practices to be applied with PcVue.

GLOSSARY

OT	Operation Technology
IT	Information Technology
ICS	Industrial Control System
POC	Proof of Concept
SOC	Security Operation Center
SIEM	Security Information and Event Management
CIO	Chief Information Officer
CISO	Chief Information Security Officer
RDS	Remote Desktop Services

1. THE RIGHT QUESTIONS TO ASK YOURSELF DEFINING A CYBERSECURITY APPROACH

1. THE RIGHT QUESTIONS TO ASK YOURSELF WHEN DEFINING A CYBERSECURITY APPROACH

WHY MY SYSTEM SHOULD BE SECURE? IS THIS MANDATORY?

- What are the risks inherent in the system?
- What are the legal obligations?

WHAT PARTS OF MY SYSTEM MUST BE SECURE?

- What is the functional and technical scope expected ?
- What requirements apply?

I NEED EXPERTISE

- What support offers exist?
- By qualified audit service providers
- By the publisher

WHICH FEATURES ARE ESSENTIAL?

- What are the possibilities for the software already in place?
- What features for an existing project?

HOW TO GUARANTEE THAT MY SYSTEM IS SECURE?

- Are the elements of the system secure?
- Is certification possible if necessary?

2. WHY SHOULD MY SYSTEM BE SECURE ?

2. WHY SHOULD MY SYSTEM BE SECURE ?

- SENSITIVE SYSTEMS, REAL RISKS
- CHARACTERISTICS OF INDUSTRIAL INFORMATION SYSTEMS
- MYTHS AND REALITIES

Supervision solutions are implemented in project contexts and sensitive operating conditions, whether for the conduct of automated processes or systems involving the safety of goods and people.

IP convergence facilitates the integration of heterogeneous equipment, interopérabilité and the deployment of supervision systems, but in return provides security risks if the project methodology and the products used do not include the "security" component. In addition, the evolution of the architectures integrating connected objects, mobility and increasingly open and interconnected systems, lead to new threats that make cybersecurity essential.

SENSITIVE SYSTEMS, REAL RISKS

All industrial and automated installations have quality of service constraints and productivity, which makes them sensitive to all disturbances (external attack, involuntary negligence or simply a vulnerability of the system) which can have real consequences.

12 INDUSTRIES OF VITAL IMPORTANCE DIVIDED INTO 4 CATEGORIES

HETEROGENEOUS INSTALLATIONS

Food Water Management Health	Civil activities Judicial activities Military activities	Energy Finance Transportation	Communications electronics, Audiovisual, Information Industry Space and research

SIGNIFICANT RISKS

- Variety of attacks
- Human error
- System vulnerabilities

REAL IMPACTS

- Safety of people and goods
- Public health risk
- Environmental risk
- Accidents, intrusions
- Harmful actions
- Operate the state's ability to act
- Denial of service
- Economic risk
- Intellectual property
- Data leak

CHARACTERISTICS OF INDUSTRIAL INFORMATION SYSTEMS

The information systems of industrial systems are distinguished from information systems of management through a number of specificities that need to be identified in order to understand the importance of securing them.

System goals

Manage physical facilities (physical, concrete)
Regulate processes
Acquire and process data

Functional aspects

Business constraints
“Real-time” constraints,
Operational safety constraints
High availability

Stakeholder culture

Automation professionals,
Electrotechnical Instrumentalists
Process engineering specialists

Heterogeneous components

The long lifespan of our facilities means that successive waves of technology are superimposed on the same site

Environment physical

Production workshops: dust, temperature, vibrations, electromagnetism, products harmful nearby, external environment, etc.

Geographical location

In warehouses, factories, on the way public, in the countryside (stations of pumping, electrical substations)

Incident management

The multitude of parameters and environment complexity limit the reproducibility of the incident

Life cycle

More than 10 years
(up to 40 years)

MYTHS AND FACTS

“ My industrial networks are isolated, I am protected. "

Industrial information systems are often connected to networks and sometimes directly to the Internet. USB keys and maintenance consoles are also major vectors of virus propagation, including on physically isolated systems. If the insulation of industrial networks is imperative, it is not sufficient and has to be complemented by other means.

" I'm using protocols and proprietary databases, I am protected. "

Even proprietary solutions include standard components, for reasons of interoperability (and for example, the operating system) and at a lowercost. Proprietary solutions are likely to be vulnerable because they may not have been the subject of any analysis of security

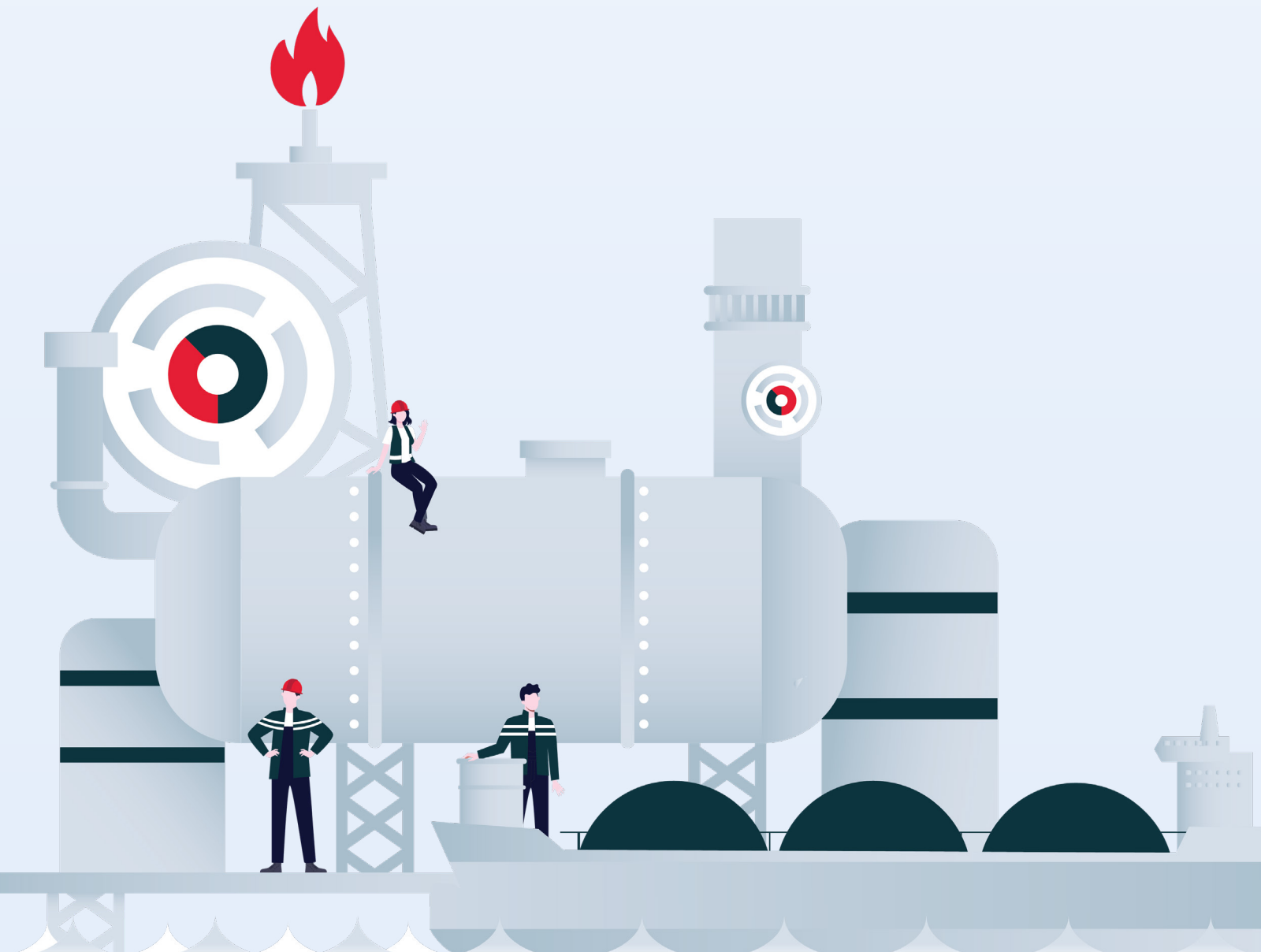
“ The integration of security mechanisms (encryption, filtering, authentication) is incompatible with the constraints response times required and the continuity of service of the industrial installations. "

The performance of the components and materials used are no longer an impediment to the deployment of security functions. In addition, the establishment of cybersecurity means it is part of an anticipated and planned approach which makes it possible to plan shutdowns without affecting productivity or process efficiency.

“ A cyberattack will always have less impact than a physical incident such as theft or fire. ”

An attack can create a global malfunction of the installations more difficult to identify and more pernicious (industrial sabotage, slowdown of production) than a physical cyberattacks can lead to a very long recovery time (several weeks).

3. GOOD PRACTICES TO SECURE SIMPLY AND EFFECTIVELY A SYSTEM

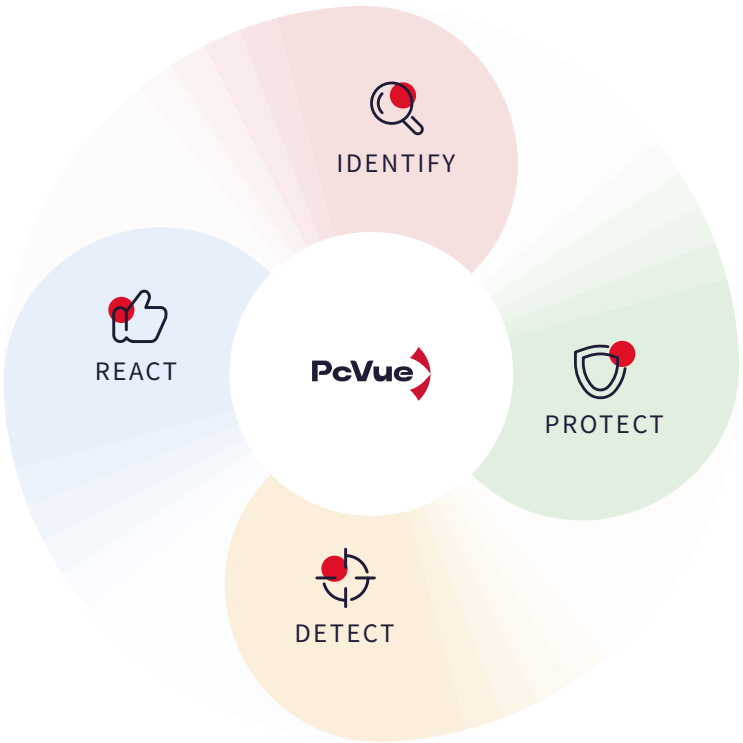


3. GOOD PRACTICES TO SECURE SIMPLY AND EFFECTIVELY THE SYSTEM

- ANALYZE THE SYSTEM - Identify vulnerabilities
- PROTECT THE SYSTEM AGAINST INTRUSIONS
- DETECT MALFUNCTIONS
- ENSURE MAINTENANCE IN OPERATIONAL CONDITIONS - Allow the resumption of activity

The PcVue supervision platform is based on devices and uses technologies that make it possible to reinforce the security of a supervision system around the 4 pillars of cybersecurity:

- System analysis and identification of vulnerabilities
- System protection to limit intrusions
- Monitoring and detection of anomalies
- Maintenance in operational conditions - Resumption of activity

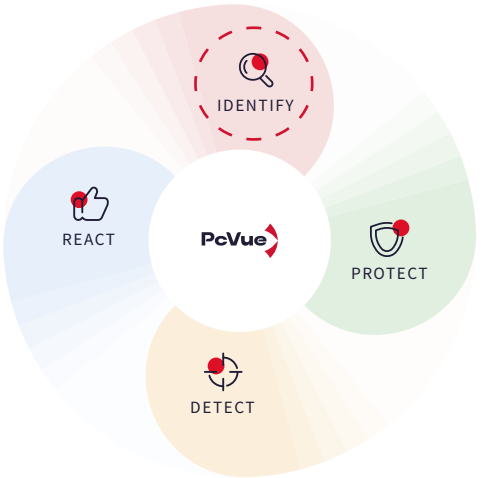


ANALYZE THE SYSTEM - IDENTIFY VULNERABILITIES

The analysis of the system and the identification of its vulnerabilities are essential prerequi-sites in securing it.

It consists of :

- Establish the security perimeter of the system and supervision system
- Define the resources required to be implemented



New systems

This study is carried out during the system design phases.

Existing systems

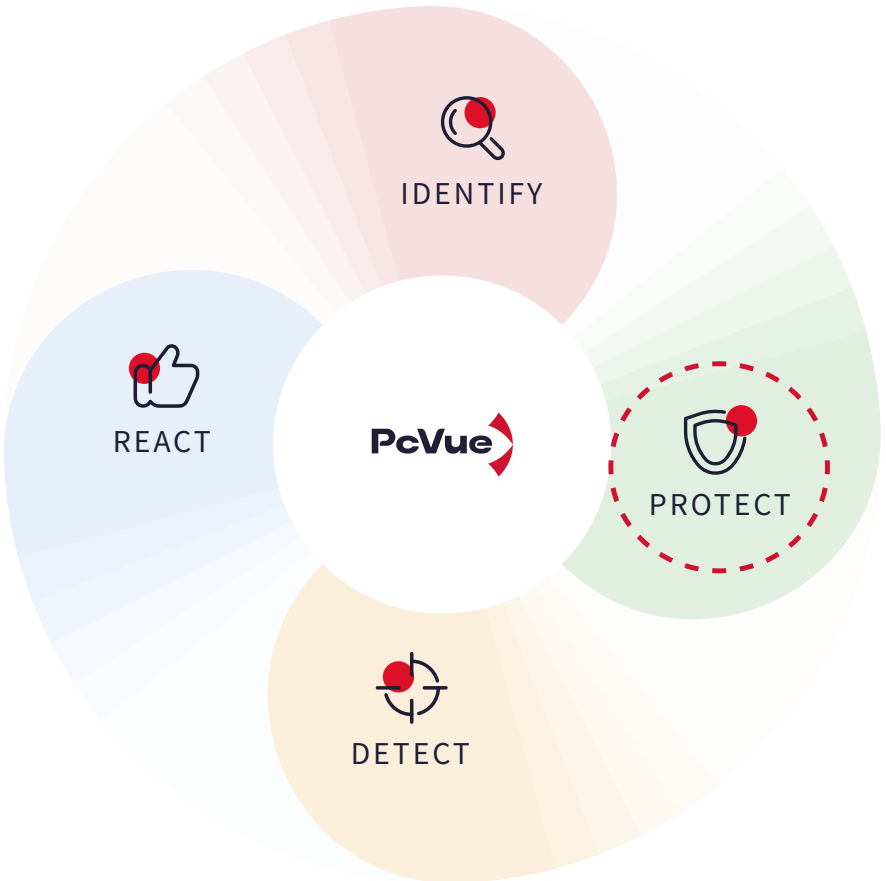
An inventory of the network infrastructure must be made. For this, a map showing network physical layout and flow logic must be established. In this context, designers must be able to rely on the various suppliers' system components such as monitoring tools. In this context, the consulting services from our “Services” offer allows you to accomplish these procedures.

TO REMEMBER

- An adapted service offer will guide you in this approach

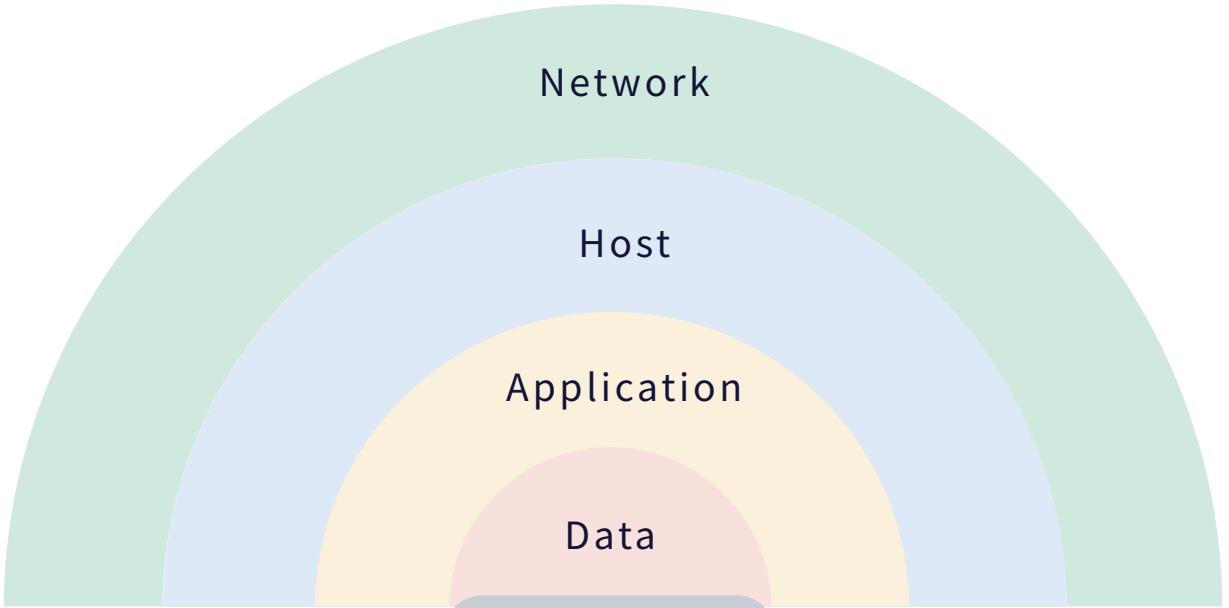
PROTECT THE SYSTEM AGAINST INTRUSIONS

Deep knowledge of the system and its points of vulnerability allows the system administrator to know what needs to be implemented for the protection of his system, a major pillar in computer security. Our solutions offer a variety of protection methods.



FUNDAMENTAL PRINCIPLE: IN DEPTH DEFENSE BY SECURITY LAYER

System protection is based on the fundamental principle of in depth defense, which consists of applying successive layers of security within the system.



Apply multiple security layers between the system and the attacker

If one of the layers is failing the others continue to operate and protect data

Securing

Coded
Equipment
Data
Transactions
Organizations

Protect a system against any type attack using independent methods

And at all levels...

CAN YOU TRUST THE SOFTWARE YOU INSTALL?

Even before using the software, make sure that it is authentic and was created by the publisher. Ensure that it conforms to the original form such that its integrity is not compromised and its components have not been altered. This constitutes the first security layer.

Since version 11.2, packages installation and binaries of PcVue are digitally signed, which guarantees you both the integrity and the authenticity of the files. This is true both during installation and later during execution.

To facilitate the distribution of our software, PcVue is available as a whole download via server FTP. We are aware that this very practical service, however, requires taking some safety precautions, such as using a server which only accepts secure FTP connections.

In addition, in order to allow you to verify the integrity of downloaded files from our server, we provide you the unique signature called “hash” of all downloadable software components. We use this method to ensure that the downloaded files are exactly as we produced them, The"hash" will not match if files have been modified or damaged. From PcVue 11.2, we use the SHA-algorithm 256 which is one of the most used for this type of verification.

TO REMEMBER

PcVue guarantees the authenticity and integrity of the installation

Secure downloads

- Access to the server by secure connections

Authentication and integrity

- The files you install have been created by the publisher and are digitally signed
- Verification of the integrity of downloads by SHA-256 algorithm

Secure installation

- Signature of installation components
- Signed binaries

WHAT PRECAUTIONS SHOULD BE TAKEN TO SECURE MY PROJECT UPON INSTALLATION?

When installing the software, the question of the functions that will be used must be considered. In fact, the installation of certain components may expose the software to attacks. It is therefore necessary to reduce the surface of exposure by installing only the necessary components.

PcVue allows during its installation to choose the components to install such as:

- Data acquisition component
- Configuration files
- Web components
- SDKs and APIs
- …

Application projects and object libraries must be deployed by secure media (white station) external to the operating network. A function of integrated version management available in PcVue will ensure the deployment of a single project version and reference libraries, on all architectural elements. PcVue constantly checks the version used on each station and alerts the operator in the event of a discrepancy.

TO REMEMBER

During installation :

- Install only the components needed for the project
- Deploy projects and libraries via secure media (white station) external to the operating network
- Use the reference version on all workstations

I HAVE TO MAKE SURE THAT THE SYSTEM MEETS THE IT PREREQUISITES

Supervision software like PcVue is used in IT infrastructures which require the conformance of a certain number of requirements, for the security of the system. Adapted deployment and tools are essential elements to take into account.

ADAPT THE DEPLOYMENT ACCORDING TO THE NEED

PcVue solutions offer various deployment possibilities to meet current constraints, while maintaining a high level of security.

CHOOSE THE APPROPRIATE EXECUTION MODE

Windows allows software to run as a service or as an application. The mode of execution as a service is appropriate for software that must run in continuously over long periods without needing user interface and not requiring intervention. Monitoring software like PcVue this corresponds to the operation acquisition server workstations or historical server. Execution mode as an application is suitable for operational use by a user through a graphical interface. This corresponds to PcVue client workstations. The advantage of using either of these modes is to be able to isolate specific server functions without a user interface from client functions with an appropriate level of security.

TO REMEMBER

Deploy server workstations as a service, client workstations as an application.

WEB & MOBILE DEPLOYMENT

Solutions for deploying different types of thin clients such as web clients or mobile applications must integrate all the functionality necessary security (https, Oauth, certificates, HTML5) as well as tools of maintenance. The deployment of these solutions also requires an architecture secure network described elsewhere in this document. PcVue web and mobile solutions operate in client/server mode, and rely on the IIS component of Windows, taking advantage of the associated protections

PcVue natively integrates a deployment console web to define, deploy and manage a web or mobile architecture.
It supports the following features:

- Deployment of web services and web applications on IIS
- Data protection management
- Certificate management
- Registration of user access and OAuth server management
- IIS audit / diagnosis

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

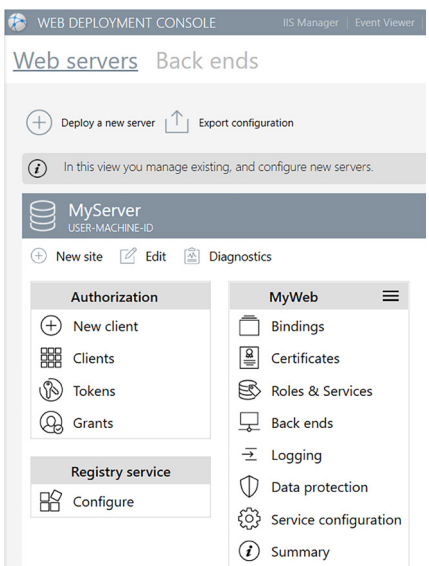


Figure 1 - Web deployement console

TO REMEMBER

Web and mobile deployment requires the following:

- Implementation of the HTTPS secure exchange protocol
- The use and management of security certificates
- Compatibility with OAuth
- A console allowing configuration, maintenance and diagnosis.

VIRTUAL ENVIRONMENTS

In addition to the standard client/server architectures of PcVue, our products are used under virtualization environments like VMware® and Hyper-V™.

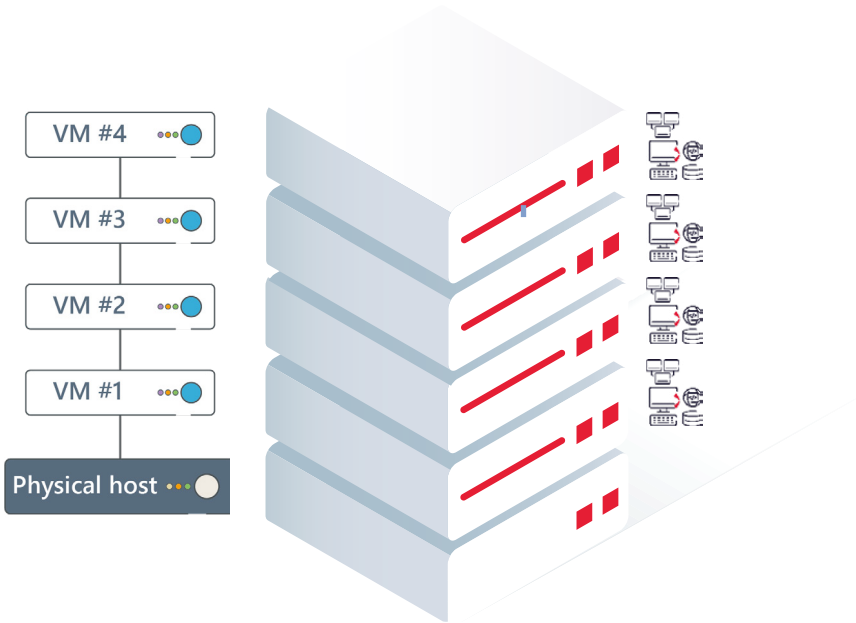


Figure 2 - Virtual environnement

These environments make it possible to operate several PcVue application servers with different operating systems on a physical unique PcVue machine.

This machine can thus be hosted in a secure computer room and backed up electrically, which will avoid geographic proliferation within of the PC client infrastructure and will thus limit the vulnerabilities for physical access to material resources, while guaranteeing the continuity of the same level of services and availability of the PcVue application.

TO REMEMBER

Deploy a virtual environment to:

- Centralize server management in a single secure location
- Limit security breaches related to physical access machine resources.

WINDOWS REMOTE ACCESS DESKTOP

Remote Access Desktop (also known as RDS) is a Windows feature which allows you to host an application on a server and run it remotely on a smartphone, tablet or PC on which it is not installed.

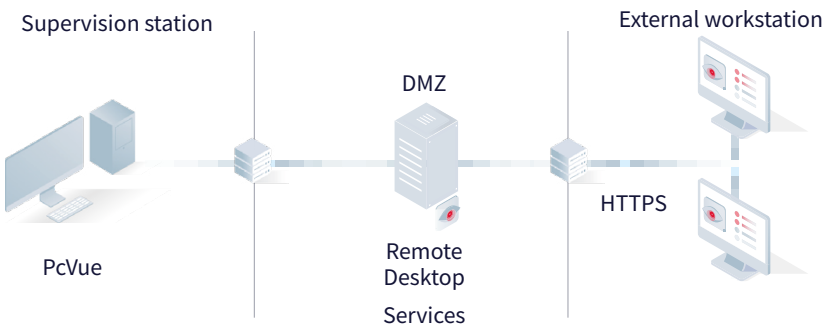


Figure 3 - Remote desktop architecture

This means that PcVue is installed on a server in which RDS feature is installed. PcVue is not installed on client terminals called "light clients". Such a deployment offers the advantage to centralize the management on a station centralized server whose access and maintenance will be limited, reducing security vulnerabilities.
The exchanges of data are limited to keyboard actions/mouse and use the protocol HTTPS, which reduces the risk of data corruption. Finally the functionality RDS benefits from the Windows security.

TO REMEMBER

Deploy an RDS environment to:

- Centralize server management in a single location and secure
- Secure remote exchanges with HTTPS
- Limit security vulnerabilities related to the installation
- of workstations
- Take advantage of Windows security features
- Limit the risks of corruption of exchanged data:
- Only keyboard/mouse actions transit over the network.

PUBLIC KEY INFRASTRUCTURE

To ensure data security, a public key infrastructure (PKI) must be used to manage digital security certificates that will provide:

- Management of access to data (authentication)
- Verification of data integrity
- Data privacy

These certificates are particularly useful for certain secure communication protocols as OPC UA, or IEC 62351 for ICCP. Generally, users of supervision are dependent on IT services for the administra-tion of PKI. In order to allow users to be autonomous PcVue provides a PKI integrated to create and deploy certificates.

TO REMEMBER

Securing data requires an infrastructure to public key (PKI) PcVue provides an integrated PKI to autonomously manage the necessary security certificates.

DOES THE ARCHITECTURE ALLOW THE SECURITY OF THE DATA EXCHANGED ?

The network architecture must be designed to secure the exchange of data, i.e. say to ensure that accesses are strictly defined and data flows controlled according to the nature of the networks.

Thus, external stations (administrative networks, internet) must not be able to direct access to industrial networks on which equipment is located.
Classically, an acquisition server station must be isolated from other networks because it is directly linked to the equipment and represents a point of vulnerability.

For this, the recommendations below should be followed:

SEGMENT NETWORKS BY SETTING UP ROUTERS
- Separate physical networks, separate logical area (VLAN)
- Use of DMZ to isolate networks and avoid unwanted intrusions
- Use of tunneling solutions to protect traffic between 2 zones

FILTER DATA BY INSTALLING FIREWALLS TO CONTROL DATA FLOWS, ESPECIALLY FROM THE OUTSIDE TO THE INSIDE OF THE NETWORKS
- Filtering of incoming/outgoing traffic by source address: destination, protocol, port

SÉCURISER LES DONNÉES ÉCHANGÉES Secure data exchanges
- HTTPS exchanges
- Use of open protocols integrating security functions
(OPC UA, SNMP v3, IEC…)

PcVue offers the possibility of designing multi-station client/server architectures on an Ethernet network using inter-station messaging based on the standard TCP/ IP layers.
On the other hand, on an existing client-server architecture, the addition of a PcVue workstation, with an identical version and having the project application set, will be impossible. The station will not be able to connect to existing stations until the administrator of the project has explicitly declared this new position and the relationships that must be maintained within the application.

PcVue is a very flexible and scalable platform allowing a multitude of architectures.
The diagram below shows an example of a possible architecture.

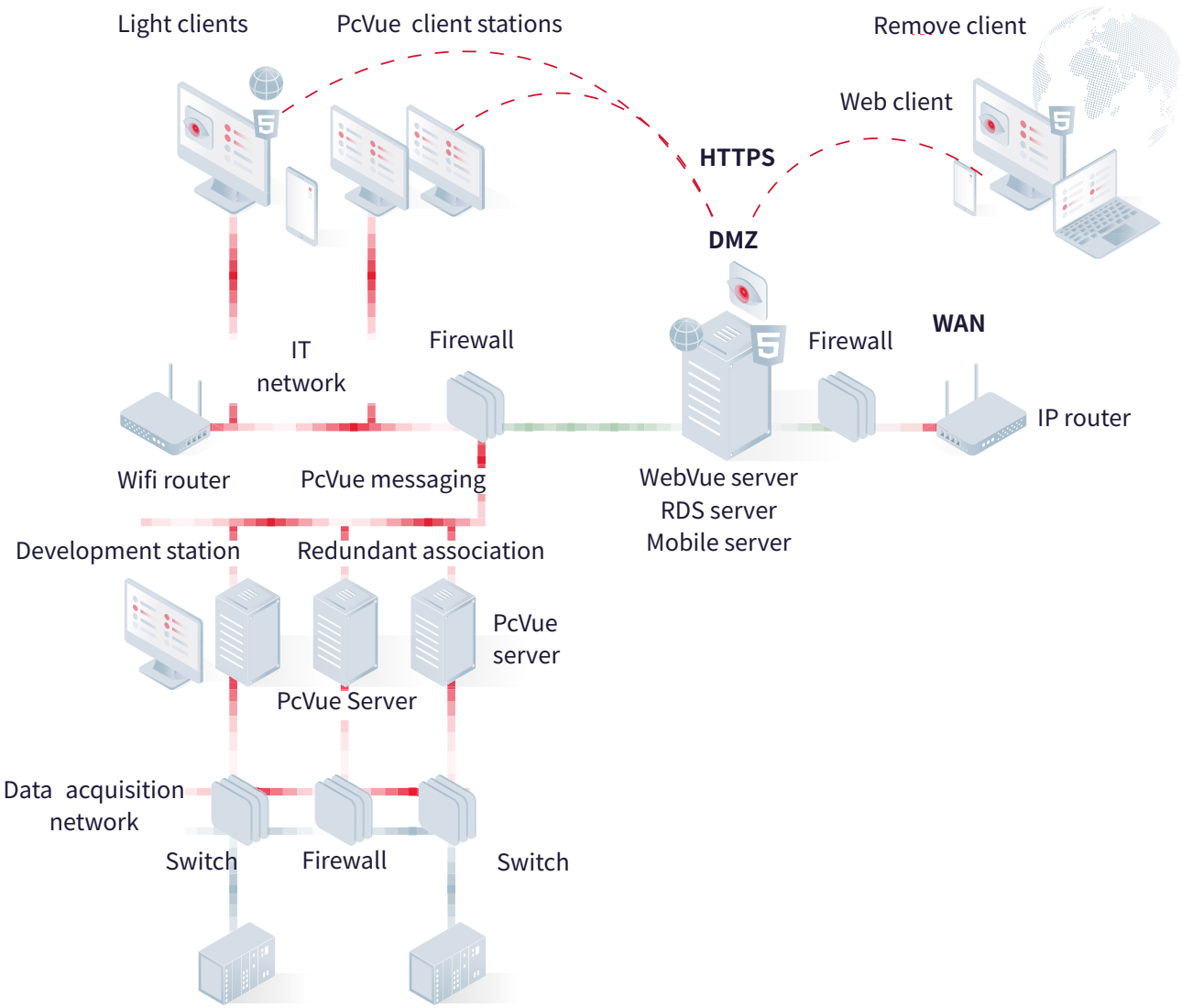


Figure 4 - Architecture's example

This sample architecture is built around the following elements:

- Data acquisition is performed by redundant acquisition servers on the industrial network.
- A development station is used for centralized management of the project. In an architecture to be approved, it is requested to isolate this station and to use a specific certified secure non-corrupt media to deploy a version project reference.
- Operation is carried out by client workstations on the isolated computer network through a firewall.
- A computer installed on a Windows server located in a demilitarized zone (DMZ) isolated by firewalls, hosts a web server, a mobile server and a server with Windows Remote Access (RDS)

- Clients can be run remotely through RDS instances using the Windows Remote Access desktop.
- An interface installed on the server allows the display of client instances on all terminals supporting HTML5.
- Web clients allow operation from a standard web browser.
- A mobile application connected to the mobile server is used for notification and acknowledgment of alarms and control from a smartphone or Tablet.
- Exchanges between the web server and the terminals use secure sockets under HTTPS.
- User access to the entire system is managed by Windows Active Directory allowing single sign-on (SSO) .

PcVue in partnership with ALLIED Telesis, offers a complete protection solution hardware to address the issues mentioned above:

- Full range of secure industrial Firewall/VPN
- Limitation and control of traffic between different areas of the network
- Creation of traffic restrictions

TO REMEMBER

- Segment networks with routers
- Filter data
- Use “tunneling” solutions: Encryption and authentication
- Secure data exchanges with firewalls
- Isolate servers in a demilitarized zone (DMZ).

SECURING SUPERVISION OF INDUSTRIAL AND AUTOMATED SYSTEMS

Data exchange between field equipment and acquisition servers presents special risks that must be taken into account in a monitoring system.

The variety of protocols used, their different modes of operation, and the nature (proprietary, or standard) does not make them equal in the face of current threats. The oldest protocols are often unsuitable for security constraints. Conversely, recent protocols often taken from international standards have necessary security features.

Whenever possible in terms of interoperability, PcVue integrates the safety features of industrial communication protocols:

- OPC UA (OPC-Security support for authentication and authorizations) and the deployment of certificates with the integrated PKI
- SNMP - PcVue's SNMP Manager implementation supports SNMP v3 which allows authentication, integrity guarantee and encryption.
- IEC protocols
- MQTT (Through TLS)

The same recommendations on securing networks apply for field networks (segmentation, filtering).

TO REMEMBER

- Favor the use of protocols integrating mechanisms of security
- Apply segmentation and filtering between networks automata between IT/OT networks
- Use routers and VPN tunnels for acquisition flows

SAFETY AND HOW TO ENSURE THE INTEGRITY OF ARCHIVED DATA?

The historical data produced by the supervision becomes more and more critical and strategic within the organization of a company. Some lessons are:

- traceability requirements
- a good understanding of the process and its analysis
- optimization of the operation or infrastructure
- analysis after incidents including potential third-party analysis.

On the other hand, the data produced and histories can reveal the characteristics manufacturing, core business company, or confidential information.Faced with the cybercriminal threat principles of production and access to historical data relies on safeguards active in our product:

- Filtered and restricted data access according to user rights
- Production of data according to different formats (proprietary and not accessible by third-parties, database SQLServer, …)

Data security and integrity can be reinforced by the devices standards offered by Windows Server and SQL Server in effect within organisation.

For example :

- User authentication, that SQL Server handles as an object "connection". Thus, only applications using these connections will have the right to use the instance. In the other case, the application is rejected from the system.
- When the connection is created, the administrator can assign rights on administration of data. To do this, SQL Server offers a range of scenarios called "Server Roles".
- When a connection is created, it alone cannot access the resources of the database engine (bases, tables, functionalities,...), it is necessary to associate it with a user of the database(s) concerned by connection. Once the user created, it is essential to attribute to it roles that will define the authorized fields of action (management of connections, backup, read access - deletion – modification, etc …)

TO REMEMBER

- Access to data filtered and restricted according to user rights
- Production of data in different formats (proprietary and not accessible by third parties, SQL Server type database, etc.)
- Security and data integrity reinforced by standard devices offered by Windows Server and SQL Server

WHAT ARE THE SYSTEM USER REQUIREMENTS?

User rights management is essential in the protection of the system of supervision because it allows control the scope of actions of the users. The characteristics of an application PcVue, for example, depend on user rights of the operator who is connected. Before using PcVue, a user must connect by identifying themselves with a name and a corresponding password to an account. The configuration of this user account determines the characteristics of the project available in operation (e.g. windows that the user can open) as well as access to configuration tools and to the operating system.
The user account can also be used to provide a selection windows associated with the user and select a program that runs when the user logs in.

DEFINE ROLES
The first step is to define roles for each user depending on its scope of action in supervision (administrator, developer, operators,…)
In PcVue, each user account is associated with a name and a password password used for login and a profile that defines the rights. There is no limit on the number of users configured but only one user can be logged in at a time on the same post. Depending on the station from which the user is logged in, the rights applied may vary. Configuration of zones is also possible. Of the zones can also be configured. Profile configuration provides user access rights. The same profile can be associated with several users. There is no limitation to the number of configured profiles. When a new user is created, a profile is associated with it.

OPTIMIZE RIGHTS MANAGEMENT
It is then necessary to optimize the management rights by selecting the options available:

- User auto-disconnect.
The time-out after a period of inactivity is configurable
- Configuration of a validity period for passwords
- Password robustness check

- Levels of hierarchical and profiles

- Locking of access to particular mimics, to command variables, or archived, acknowledgment and masking of alarms, etc.
- Configuration of different profiles for a user depending on the workstation on which he is connected, in a multi-station architecture
- Password change on first login
- Management of the "quarantine" of a user after three attempts to unsuccessful connections
- Encryption of user account information

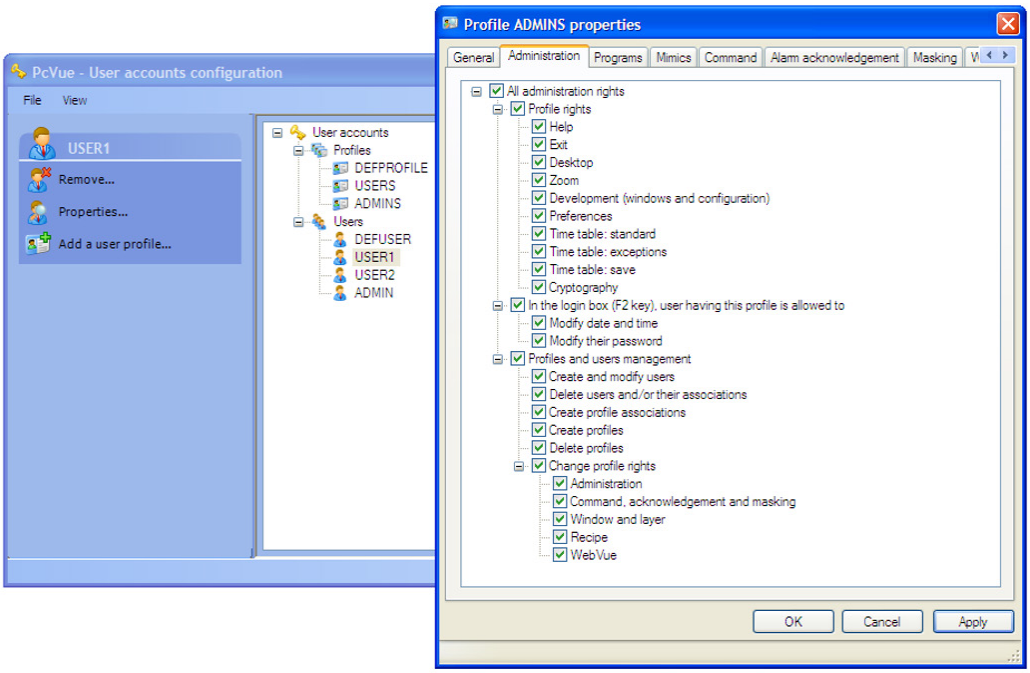


Figure 5 - Configuring user profiles

Use Rights Management and Company Directory

Some companies impose within their I.T. architecture to have only a central directory listing all the potential users of their resources computers. PcVue makes it possible to rely on the Windows Active Directory to ensure user identification and authentication.

In this case, users are not declared directly within the Supervisor, but the "PcVue Profiles" "association" and "Active Directory Groups" allows PcVue to determine permissions and user privileges within the supervision application, such as the rights control (command, instruction), or the rights of acknowledge of alarms (by level, priority, etc.). These principles of exchange are completely automated and transparent at the operating level. You should also check the directory encryption.

CHOOSE THE RIGHT LICENSE MODE

Regardless of user rights, changes can be made at the project configuration level only if the PcVue licenses include the development mode. Logically, "runtime" licenses do not in any way allow access to the product configuration menus. This principle reinforces restriction of the capabilities of modification of the application by deploying only licenses of this type.

These principles are reinforced by the management of user rights since even if a person accesses the station with a protection key allowing developments, if the latter does not have the necessary profile and password, he will not be able to access the development functionality of the project.

Map and track user accounts
It is imperative to have a vision of the users of the system and in particular of the users assets. Unnecessary accounts or profiles should be deleted. Generic accounts (an account for a team, for example) should be prohibited. The user activities may be logged in order to be able to understand the progress of events in the event of an incident or attack.

TO REMEMBER

- Define roles
- Map and track user accounts
- Optimize rights management
- Use company directory rights if possible
- Check directory encryption

TABLE OF AVAILABLE SECURITY FUNCTIONS IN PCVUE

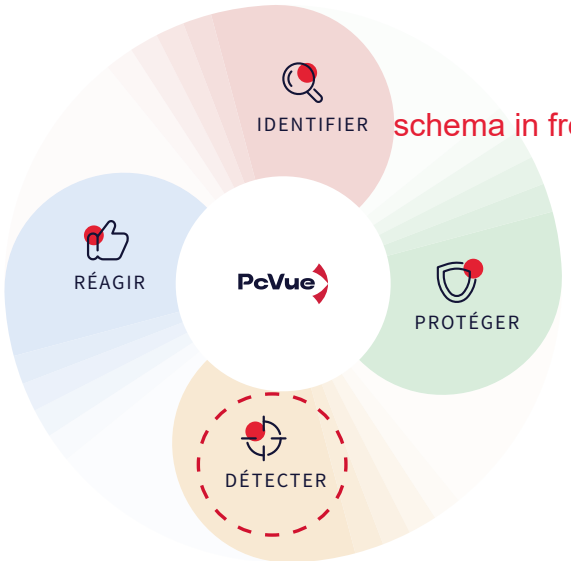
In the French version the left & right of this sheet doesn't have the same font..which is better and clearer

FUNCTIONALITY/TECHNOLOGY SUPPORTED	COMMENTS
Secure HTTP (HTTPS)	WebVue and WebServices are proxy-aware interfaces
Proxy	It is possible to use the mechanisms PcVue authentication or delegate LDAP authentication using Active Directory only.
Ability to disable or uninstall features or unused interfaces. By example: Telnet, FTP access, WEB Interface, Protocols control command, Interface serial, USB port ...	Most optional features may already be deactivated or blocked. The default configuration new versions is more restrictive in order to improve security.
Public key infrastructure (PKI)	Integrated PKI support

Figure 6 - Table of available security functions

DETECT MALFUNCTIONS

When the steps of identification and protection have been carried out, it is necessary to check that the system works as it should and detect abnormal behavior relative to a reference state.
PcVue offers various ways to monitor the state of health of an installation, both in terms of applications and networks and relies on many tools for monitoring and diagnosis of a supervision system.



schema in french

HOW TO DIAGNOSE OPERATION OF THE SYSTEM?

AUDIT DIAGNOSIS

The "diagnostic audit" is a PcVue component that allows you to view information relating to the internal functioning of the supervisor. Its main use is a diagnostic aid but it can also be used to check the good general functioning of a system. Two tracking pages are available:

COUNTERS AND MONITORING

This view provides a detailed list of counters internal to the supervisor.

Object - Counters for system resources and application objects.
Instance - Message counters between PcVue handlers and the memory allocated to them.
Time - Time spent processing messages at each handler.
Flow - Data flow associated with real-time value transitions of variables in the variable tree.

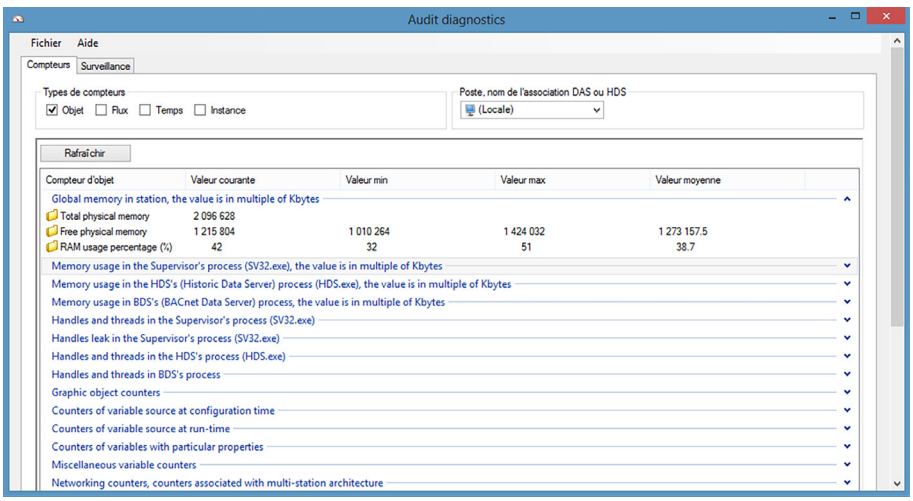


Figure 7 - Diagnostic tools

MONITORING

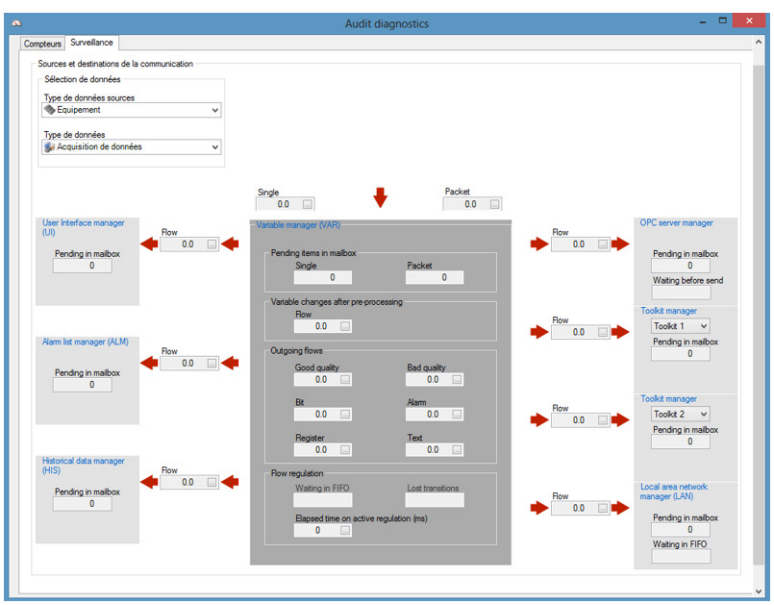


Figure 8 - Visualization of flows

Flows visualization

This view allows the user to have an instant vision details of exchanges between the different modules internal PcVue and to have detailed information on the corresponding data streams at transitions real-time value of the variables.
Thus, the user is able to analyze the state of health of the system. Two views are available: one displaying the data acquisition flow (incoming data in PcVue) and the other displaying the write stream (data sent from PcVue).

SECURING SUPERVISION OF INDUSTRIAL AND AUTOMATED SYSTEMS

EVENT LOGGING

PcVue has a data recording module for events such as alarms, operator actions, or value changes. These events archived files can be displayed to operators using a consignment.

SYSTEM VARIABLES

PcVue offers a large number of system variables indicating the operating state of the supervisor (number of requests in progress, pending, archived flow, etc.).
This data can be viewed in multiple forms (instantaneous values, meter view, curves, etc.) in supervision synoptics and archived if necessary. In addition, they can be transmitted to a third-party supervision system, thanks to the PcVue SNMP Agent protocol.

EVENT LOGS

All PcVue modules generate traces collected in event logs. These logs, stored as local trace files, can also be centralized within a SIEM (Security information and event management). This logging is useful in all cases where post-mortem analyzes must be carried out: dysfunction of the system, suspicion of intrusion…

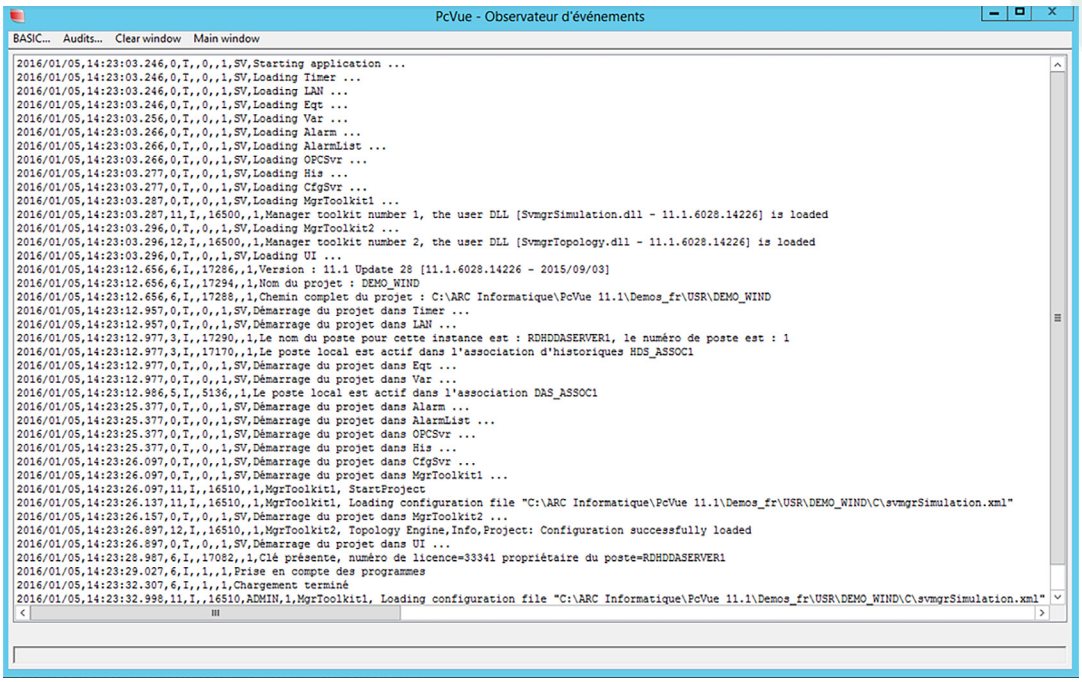


Figure 9 - Event Viewer

I MUST PROVIDE THE ANALYSIS OF THE REPORT FOR INCIDENTS TO IT MONITORING TOOLS

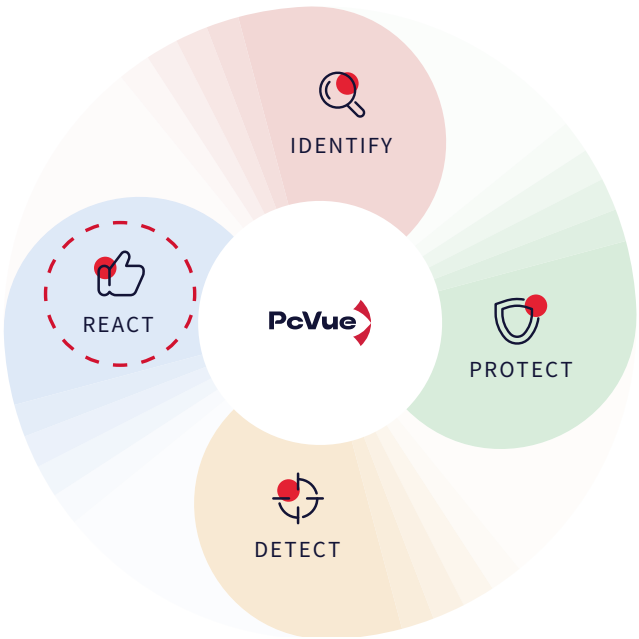
SYSLOG and Windows Event Logs

PcVue allows event logs to be aggregated by monitoring tools of third-party computer systems for the correlation and analysis of events: PcVue supports Windows Event Viewer and SYSLOG over UDP, TCP and TLS - RFC 3164 and 5424 and complies with ANSSI and IEC 62443 requirements for logging and tracing

TO REMEMBER

- Verify system operation with built-in audit and diagnostic functions
- Consult the traceability tools
- Share system data to IT monitoring tools

ENSURING MAINTENANCE IN OPERATIONALCONDITIONS - ALLOWING THE RESUMPTION OF ACTIVITY



PcVue natively integrates an advanced project version allowing restore appropriate behavior application after an incident. "Project version management" relies on a configuration repository. It allows management of an access point where the entire dataset "application" (object library, database setup, user rights, etc.). Reinforced by Microsoft Windows server. This will limit access to this information only to persons authorized to modify the characteristics of the app. Usually a dedicated development station of the PcVue SCADA application is used to host the project version in a central directory and make changes to this project. In an architecture to be certified, it is required to isolate this workstation and use a specific secure media certified as uncorrupted to deploy a reference version of the project. In addition, to ensure the integrity of data and operating reliability of the process. We complete application management principles by providing traceability based on the management of the version. Thus, you can preserve and protect all of the dataset of its application

For example :

• The N-1 version, in order to be able to problem very quickly come back on the previous version
• Version N in operation, previously been the subject of all qualification phases and verification
• The N+1 version(s) in progress development that has been thesubject or not qualification and verification phases

A comment box allows you to specify status or information necessary for the version situation and allows the traceability of modifications.

Version management will allow for deployment aspects:

• Automatically broadcast to all architecture posts new data set to ensure data integrity and consistency exploited
• To any new workstation declared in the architecture to download the reference version, without fear of exploiting an unvalidated or outdated dataset
• At any station temporarily stopped, from its start-up phase to check if the project version he has is well the current version, what in it will automatically download
• The N-1 version, in order to be able to problem very quickly come back on the previous version of the reference version.

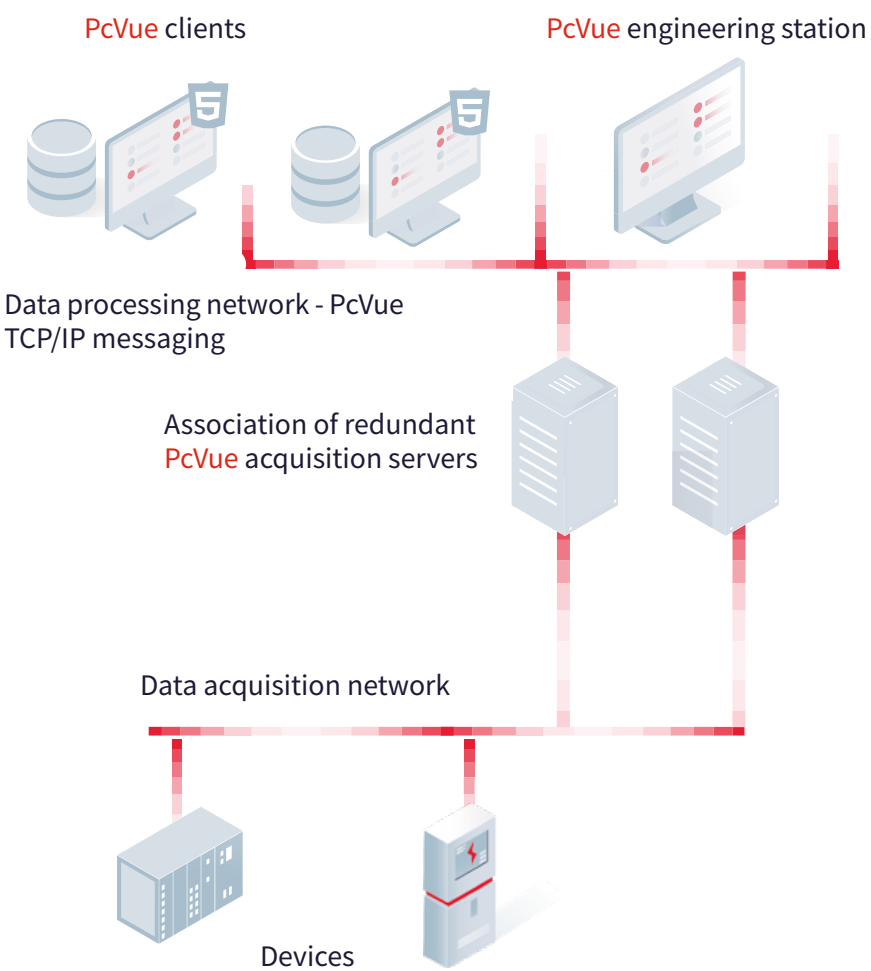


Figure 10 - Architecture with centralized version management

4. ARC'S COMMITMENTS FOR CYBERSECURITY

ARC'S COMMITMENTS FOR CYBERSECURITY

DESIGN PRODUCTS

The safety dimension largely depends on the conditions in which our products are designed and developed.

This is based on certain principles:

Design, development, qualification and production processes resulting from our ISO 9001 Quality management system including
• Specification methodology, design and development
• Verification plan
• Qualification plan
• Use of software robots for unit testing
• Full-scale validation on beta sites
• Internal platform qualification on full-scale projects (load and performance measurements)
• Regression tests
• Quality system for tracing anomalies
• The company does not subcontract studies, development or qualification of these products beyond the ARC Group of companies.
• Our products have monitoring and logging mechanisms, allowing to detect any anomaly and thus facilitate the phases of customer diagnosis
• Operating statuses of the various components of an architecture, allowing the customer to know and control the behavior of his system

SECURITY AND PROJECT MANAGEMENT

As mentioned in the introduction, the security approach of a supervision project cannot be based solely on the precautions and devices introduced into the products or technologies (supervisor, Vlan network architecture, web access, etc.).

This requires that the project methodology including the phases of studies, specifications, testing and commissioning incorporates this dimension. It is the same for the operation and maintenance phases.

For this our "Services" offer we include training services, assistance, advice both in the preliminary project and in the construction or maintenance phase, which allows us to support our customers and allow them to benefit from our experience on this subject within the scope of your supervision system.

We have thus supported our clients in project contexts such as:

• Operation of energy production facilities in a nuclear environment
• Safety and the conduct of experiments in the nuclear environment (Projects SIL II classified)
• Supervision of transport infrastructures or infrastructures open to the public for safety goods and people
• Energy transport networks
• Etc …

SECURITY POLICY

Despite all the efforts made, our products may be subject to vulnerabilities likely to endanger the systems in which they are integrated. In order to minimize the impact of these vulnerabilities, ARC Informatique implements transparent practices for its customers, the authorities and the general audience.

In practice, and beyond the design phases of our products, we are committed to :

1. Make our know-how available to our customers and our partners for help with implementing secure solutions,

2. Ensure active monitoring and follow-up of alerts concerning our products,

3. Coordinate our actions with the network of CERTs – Computer Emergency Response Teams – as well as the IT security actors who adhere to these CERT commitments and recommendations,

4. Communicate transparently about known vulnerabilities in our products with security alerts – Whether they are issues discovered internally or by third parties,

5. In the event of an alert, provide security bulletins in order to bring as quickly as possible to provide our customers with information to reduce immediate risks:
https://www.pcvuesolutions.com/security

6. Take advantage of feedback to design safer products.

Sources

PcVue - Good practices of web & mobile deployment under supervision

PcVue - Architectures and deployment

PcVue

LET'S ENGINEER

ARC INFORMATIQUE

www.pcvue.com

PcVue – Securing supervision of
industrial and automated systems EN
Publication number: AT-2024-14-08 v.4

swiss safety center
ISO 9001
ISO 14001
ISO 27001
certified system