



# Web & mobiles clients for supervision systems

## Good practices guide for deployment

Author :  
François Flèche  
Marketing and pre-sales at Arc Informatique

September 2019

The information in this book is subject to change without notice and does not represent a commitment on the part of the publisher. The software described in this book is furnished under a license agreement and may only be used or copied in accordance with the terms of that agreement. It is against the law to copy software on any media except as specifically allowed in the license agreement. No part of this manual may be reproduced or transmitted in any form or by any means without the express permission of the publisher. The author and publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book. In particular, the information contained in this book does not substitute to the instructions from the products' vendor. This book may contain material belonging to third-parties. Such information is used exclusively in internal work processes and is not intended to be disclosed. In addition, this notice is not a claim of property on such third-party information.

# Content

<b>WHO IS THIS DOCUMENT FOR? .....</b>	<b>2</b>
<b>GLOSSARY .....</b>	<b>3</b>
<b>1. CONTEXT .....</b>	<b>6</b>
1.1 EVOLUTIONS OF TECHNOLOGIES.....	6
1.2 EVOLUTION OF USES.....	7
1.3 OPPORTUNITIES AND CHALLENGES .....	7
<b>2. THIN CLIENT VS HEAVY CLIENT .....</b>	<b>8</b>
<b>3. TECHNICAL PREREQUISITES FOR WEB &amp; MOBILE CLIENTS DEPLOYMENT .....</b>	<b>9</b>
3.1 DIMENSIONING OF SYSTEM.....	10
3.2 SECURING NETWORKS.....	10
3.3 HTTPS.....	12
3.4 DIGITAL CERTIFICATES.....	13
3.4.1 "Self-signed" certificate .....	14
3.4.2 Certificate issued by a domain controller .....	14
3.4.3 Certificate issued by a trusted third party .....	14
3.5 DOMAINS AND NAME RESOLUTIONS .....	16
<b>4. EXAMPLES OF ARCHITECTURES .....</b>	<b>18</b>
4.1 ARCHITECTURE #1: SIMPLIFIED « ALL-IN-ONE » DEPLOYMENT .....	19
4.1.1 Description.....	19
4.1.2 When to use this architecture.....	20
4.1.3 Benefits .....	20
4.2 ARCHITECTURE #2: « ALL-IN-ONE » DEPLOYMENT WITH INTERNET ACCESS .....	22
4.2.1 Description.....	22
4.2.2 When use this architecture .....	23
4.3 ARCHITECTURE #3 : SECURE DEPLOYMENT BY NETWORK SEGMENTATION AND DMZ .....	25
4.3.1 Description.....	25
4.3.2 When to use this architecture.....	26
4.3.3 Benefits .....	26








# Who is this document for?



---

This document provides the keys to a successful deployment to anyone who wants to set up Web or mobile clients in their supervisory architecture.

# Glossary

---

Name	Abbr./Icon	Description
Supervision system	SCADA	Software platform to monitor and control installations by visualizing, controlling and processing real-time values from equipment.
Real time data acquisition server SCADA station		Supervision station that acquires data from equipment on a field network and supplies client stations on an industrial network.
Client SCADA station		Supervisory station that retrieves data from an acquisition server station on an industrial network.
Microsoft® Internet Information Services	IIS 	Extensible web server from Microsoft bundled with Windows operating systems and used by the supervisor to provide access to web services and applications.
Web server station		Host the Supervisor web services and applications, and is based on Microsoft Internet Information Server. The web server can be on the same machine as the web back end SCADA station or on a separate one.
Web components		Set of services and applications installed on a Web server station to connect web and mobile clients to the supervisor.
Web Back end SCADA station		Supervisor station that serves as a gateway to provide the data to the web server. The Supervisor must be installed on the machine playing the role of web back end and the application must include the back end configuration. The web back end may or may not be on the same machine as the web server.
Web & Mobiles clients		Terminals running a web client in a web browser or native mobile application.
Web deployment console	WDC 	Desktop application installed on the web server station, used to deploy web and mobile clients. It makes it possible to configure all the elements necessary for the deployment of Web and mobile clients (roles, security certificates, IIS, ...) and to ensure the maintenance of the configuration (diagnostics, modifications, ...)
Industrial network		Network segments that include SCADA stations. Designated as the Level 2 Industrial Network in the ANSI / ISA-95 Information Model (also known as the SCADA Level).

Name	Abbr./Icon	Description
Field network		Network segments that include equipment and / or communicating systems.
Demilitarized zone	DMZ	A demilitarized zone is a physical or logical network that contains and exposes an organization's external services to an untrusted network, typically 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).
Domain Name System	DNS	DNS is a decentralized hierarchical naming system for computers, services, or other resources connected to the Internet or a private network.
Sub network		A subnet is a logical subdivision of an IP network. Computers belonging to a subnet are addressed with a common, identical and meaningful group of bits in their IP address. The traffic is exchanged between subnets via routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between subnets.
Virtual Private Network	VPN	A Virtual Private Network (VPN) extends a private network over a public network and allows users to send and receive data over shared or public networks as if their computing devices were directly connected to the private network.
Fire-wall		A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Network Address Translation	NAT	A method of modifying one IP address space into another by modifying the network address information in the IP header of packets when in transit on a traffic routing device. A "routable" Internet IP address of a NAT gateway can be used for an entire private network.
Certification authority	AC	Entity issuing digital security certificates
Hypertext Transfer Protocol Hypertext Transfer Protocol Secure	HTTP / HTTPS	Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative and hypermedia information systems. HTTP is the basis of data communication for the World Wide Web. HTTPS (HTTP Secure) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication, often called HTTP over TLS or HTTP over SSL.

Name	Abbr./Icon	Description
Internet Services Provider	FAI	Internet operator who provides an internet connection through a physical box commonly called box

# 1. Context

## 1.1 Evolutions of technologies

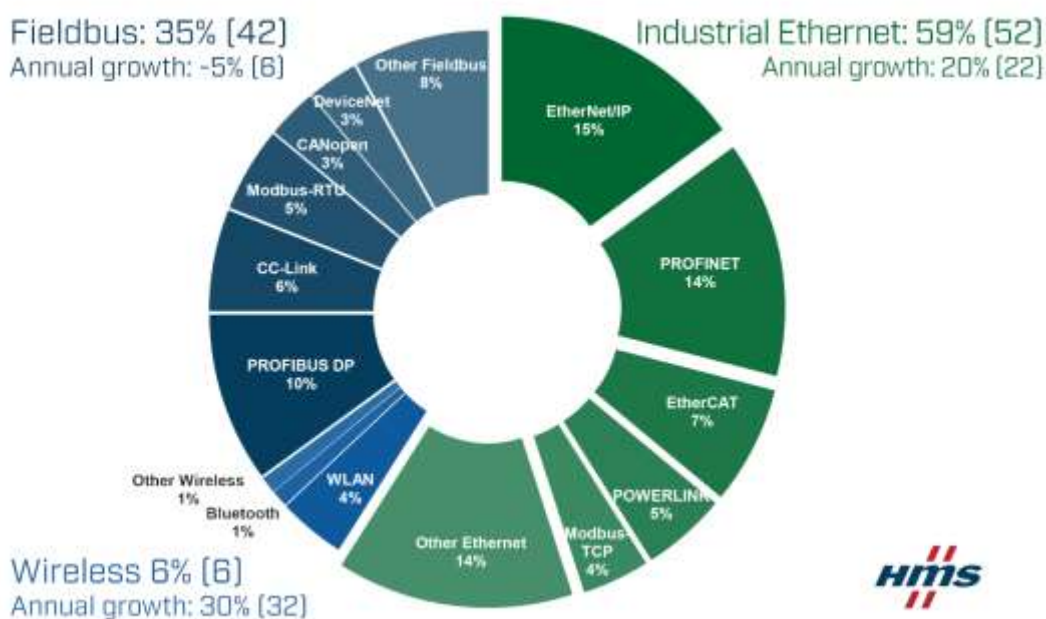
Automated systems have long been based on "closed", system-specific architectures and were by definition isolated from other systems in the enterprise.

In addition, they mainly used proprietary communications drivers to exchange data between equipment and software to supervise them.

The massive development of so-called "open" networks, that is to say more standardized and allowing connection to a wider set of systems or equipment, has had a strong impact on automated systems.

In fact, the IP and wireless networks created and used for the Internet, have gradually been adopted by corporate computer systems and then by automated systems.

Automated systems and associated equipment are currently mainly connected to "open" and wireless networks, as confirmed by a study conducted by HMS in 2019:



<https://www.hms-networks.com/news-and-insights/news-from-hms/2019/05/07/industrial-network-market-shares-2019-according-to-hms>

Figure 1 – Industrial market shares 2019

In addition, the massive adoption of mobile devices (smartphone, tablet) in everyday life, outside the industrial context, reinforces the exploitation of these solutions. Mobile devices are more and more efficient, offering computing power and display often more optimized than a simple PC.

The same goes for Wi-Fi networks, which are now reaching extremely high speeds, allowing a very smooth use regardless of the position at the heart of the plant or site.

## 1.2 Evolution of uses

These technological changes have in fact modified the possibilities offered, making accessible from outside the systems that were previously isolated and little or not accessible.

In addition to interoperability with other systems, the opening of automated systems on networks today allows operators to perform their tasks not only from a control room, but also remotely from remote offices through a web interface, or in a mobile way closer to the equipment from a remote station on site or with a mobile application on smartphone.

In terms of infrastructure maintenance, opening up to networks also implies a change in work habits, as two worlds must now work together: the operational staff (OT) closest to the automated systems and equipment and the IT experts (IT) in charge of network infrastructures.

This is an important element to take into account when choosing a system supervision software solution that must be designed to meet the constraints of each type of stakeholder.

## 1.3 Opportunities and challenges

As we have seen technological developments and the advent of networks created opportunities for better interoperability between systems, an almost infinite amount of data available, remote and mobile access to the supervision system and overall an improvement of the operation and maintenance of the systems. However, this implies precautions in terms of deployment because the risks associated with the networks are real in case of attack called "cyber".

For example, when an ill-intentioned entity accesses a sensitive equipment via a network in order to modify the parameters thereof.

The aspect of "cyber security" is therefore to be taken into account when deploying solutions based on the use of networks, especially when it comes to setting up web and mobile access.



## 2. Thin client vs heavy client

Remote supervision can be done from a so-called "heavy client" station, that is to say a station on which software is installed which connects to another station to recover the data.

Or it can be done from a "thin client" which is a terminal (PC, smartphone, tablet) on which we access the supervision either from a remote desktop session windows (RDS) or through a browser (we speak of "web client") or with a mobile application (in this case we speak of "mobile clients").

The thin client offers the advantage of not requiring installation and can therefore potentially be run from all types of mobile devices, or PCs with a minimum of constraints. In addition, it is not necessary to have a user license or a protection dongle on the thin client terminal to access the system, authentication by name and password is sufficient.

On the other hand, in the case of deploying web and mobile clients, it will be necessary to set up a web server that will bridge the gap between the main supervision server and the thin clients. Deployment and maintenance will be from this station only.

Thin clients, especially web and mobile clients, provide ease-of-use (mobility, a variety of supports) that meet the needs of users and ease of deployment and maintenance. It should be kept in mind, however, that the data used comes from a supervisory system that will have to be installed and maintained in all cases (acquisition of field data, archiving, processing, etc.) and that a minimum of prerequisites are required to deploy web and mobile clients, especially in terms of security.

In the rest of this document, we will describe the best practices for deploying web and mobile clients for a supervision system.

### 3. Technical prerequisites for web & mobile clients deployment

The deployment of web and mobile clients implies, in fact, the use of computer networks, internal to an organization with restricted access to a certain domain, or external with wider access, for example from the internet.

Above all, the deployment will depend on the sizing of the necessary architecture according to the uses: number of users, number of installations (networks, sites ...), and nature of access (internal, external access, office and industrial networks ...) etc.

In any case, it will be necessary to respect technical prerequisites in terms of security in particular, such as:

- Ensure the legitimacy of the servers
- Protect data during exchanges between servers and web clients
- Manage access to data according to areas of use

The main objective is to guard against a malicious attack that alters the data and can have serious consequences on the operation of the installations.

In other words, you have to know how to answer the following questions:

- Where do the data come from?
- Are the data the same at the start and the finish?
- Who has the right to access it and in what domain?

For this, the following actions should be performed when deploying web or mobile clients:

- Sizing of the system and networks
- Securing networks
- Implementation of an adapted domain management
- Using a secure data exchange protocol
- Creation of digital security certificates

It is clear that this approach requires IT skills but also the expertise of the automation specialists and maintenance/operation operators.

## 3.1 Sizing of system

This step will consist of defining a number of elements that will guide the technical decisions to be made. The following questions will need to be answered:

- Number of users?  
Beyond a certain number of users, the use of a server-type station will be imperative.
- Number of installations (networks, sites ...)?
- Nature of access?
  - o Internal or external access on one or more networks (industrial, office, internet, ...)

The nature of the access will have direct consequences on the technical choices. For example if an external access from the internet is planned for the web clients a VPN will have to be put in place.

## 3.2 Securing networks

The deployment of web or mobile workstations needs to follow good cybersecurity practices in terms of network deployment, ie to ensure that access is strictly defined and data flows are controlled according to the nature of the data networks.

Thus a web client must not be able to directly access the industrial networks on which the equipment is located.

Classically a post hosting the web server must be isolated from other networks because it is the entry point of requests from web clients and therefore a point of vulnerability.

For this it will be necessary:

- to set up routers to segment the networks,
- to install firewalls to control data flows, especially from the outside to the inside of the networks,
- to put the web server in a buffer zone called DMZ<sup>1</sup>.

A DMZ or demilitarized zone is a network isolated from both industrial networks and external networks. In the diagram below, given as an indication, the web client accesses industrial and field networks only

---

<sup>1</sup> DMZ : DeMilitary Zone

through the web server located in a DMZ. Firewalls handle allowed flows and filter data.

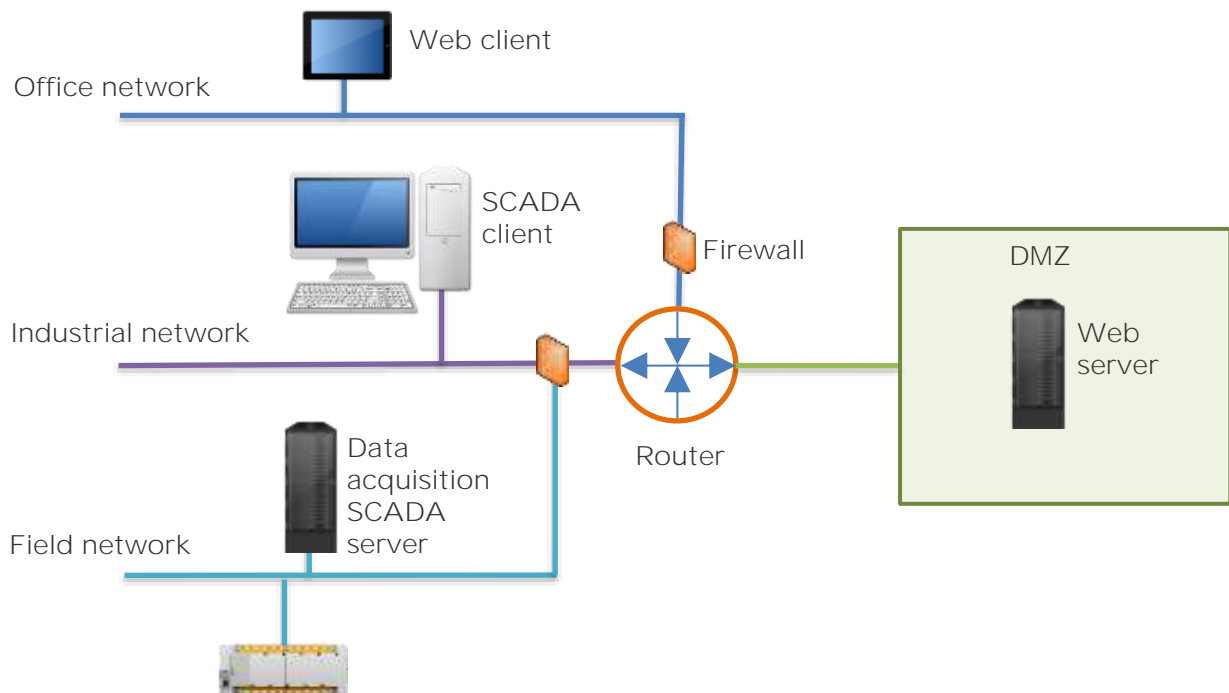


Figure 2 – Example of architecture with segmented networks

**TO REMEMBER**

### Securing networks

- ✓ Segment the different networks with routers
- ✓ Control data flows with firewalls
- ✓ Isolate the web server in a demilitarized zone (DMZ)

## 3.3 HTTPS

To ensure the identity of the server to which the web clients connect and to guarantee the authenticity and integrity of the data between the server and the web clients, the use of the HTTPS<sup>2</sup> protocol is imperative.

The special feature of this so-called secure protocol is that it uses a data encryption layer (SSL or TLS in the latest versions). This makes it possible to secure the transmission of data and to be certain that the data is identical from end to end of the exchange and to guard against data interception during the exchange.

On the other hand, HTTPS relies on the use of security certificates allowing the user, through the web browser, to verify the identity of the server to which it connects and to access the content only if the server is trustworthy.

This protocol used in web exchanges is gradually becoming the norm and replaces its HTTP predecessor that did not contain the encryption layer. If today web browsers display a simple warning message when HTTPS is not used, tomorrow access to the content will probably be blocked if necessary.

**TO REMEMBER**

### HTTPS

- ✓ Secure data exchange protocol between a web server and web/mobiles clients
- ✓ Check the legitimacy of the server
- ✓ Guarantee the authenticity and integrity of the data exchanged
- ✓ Requires the use of security certificates

---

<sup>2</sup> HTTPS : Hyper Text Transfer Protocol Secured

### 3.4 Digital certificates

A digital certificate is a way to verify the identity of an entity (i.e. a web server) and to guarantee its authenticity.

It contains information about the entity (Name, address, period of validity ...).

It is tamper-proof (encrypted), nominative (issued to an entity) and certified (by an encrypted signature).

Typically, when a web client tries to access data on a web server, the browser checks the certificate issued by the web server before granting access to the web client.

In this case, it answers the question:

"Can we trust the web server? If the answer is no, the browser will display a warning message before displaying the content.

There are three levels of certificates that should be chosen according to the context of use.

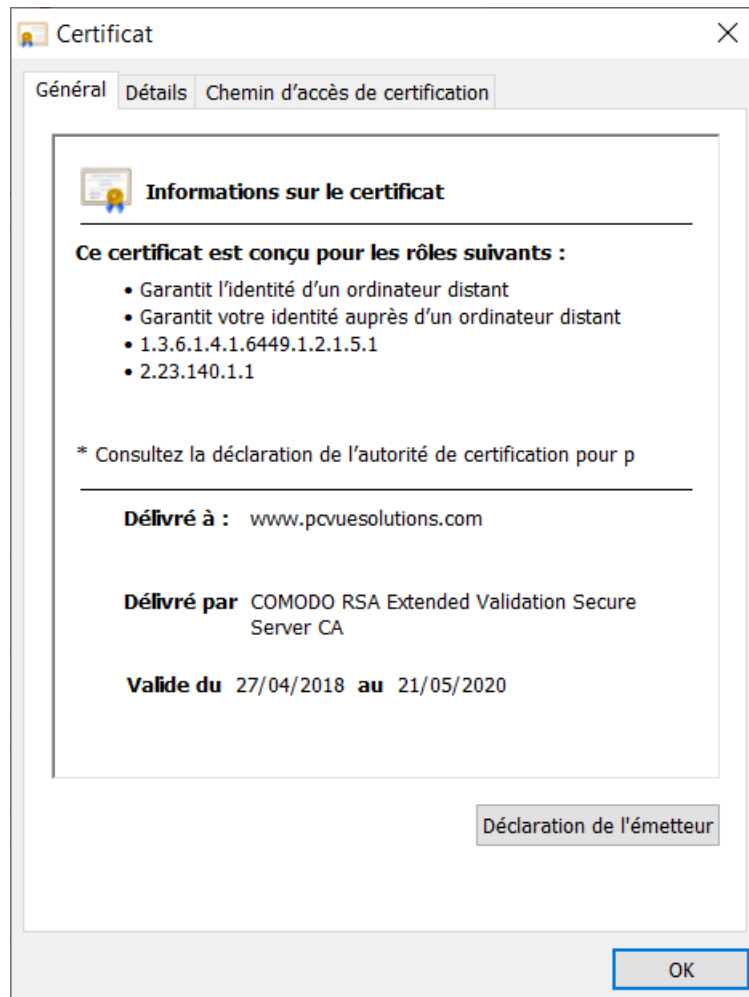


Figure 3 – Example of digital certificate

### 3.4.1 “Self-signed” certificate

This certificate is issued by the user himself and therefore commits only his own responsibility. It will allow a web client to access the content but, not being issued by an independent authority, the browser will display a security message.

On the other hand, private keys used for encryption and authentication are more vulnerable to a spoofing attempt in the case of a self-signed certificate as handled locally.

This type of certificate should therefore be reserved exclusively for testing or development phases on the same machine and not for access from private or public networks.

### 3.4.2 Certificate issued by a domain controller

In the case of an internal network controlled by a domain server, it is possible to create a certificate issued by the domain server.

The server and the web clients on the same network administered by the IT certificate guarantees trust within the organization.

The advantage of such a certificate compared to a "self signed" certificate is that it will be recognized as secure by browsers and will not display an alert message. It also ensures secure management of encryption keys by the domain controller that issues it.

### 3.4.3 Certificate issued by a trusted third party

In the case where web clients are on an external network, in particular the internet, whose access is open to users who are not part of an internal organization, it will be necessary to choose a certificate issued by a certification authority (AC). CA is a trusted third party that offers the highest level of certification and control.

TO REMEMBER

### Digital security certificates

Used to verify the identity and authenticity of a web server

### Self-signed certificate

Security Level: LOW / **Alert Message Displayed When Accessing Content**

Usage: Development / Tests on a single machine

### Certificate issued by a domain controller

Security level: HIGH

Usage: Internal network with a domain controller administered by an IT team

### Certificate issued by a certificate authority

Security level: HIGH

Usage: External network with public access (internet) not administered by an IT team



## 3.5 Domains and Name Resolutions

A station hosting a web server, like any machine in a network can be identified in different ways. By default, it is identified by its IP address or the name of the machine.

It can also be identified by a domain name that is managed by a DNS<sup>3</sup> server. The role of a DNS server is to do the name resolution, that is the link between the IP address of a machine and a name, on a private or public domain. Besides the fact that it is easier to enter a name rather than an IP address, the name offers the advantage of remaining identical even if the IP address of the host changes.

The use of the https protocol and associated certificates requires identification either by hostname, in a Windows private network (with DNS if non-Windows terminals are to be used), or by domain machine name, assigned by a Public DNS, in the case of a public network (without VPN). In any case, the use of the IP address or the machine name will cause the display of an alert message before accessing the content.

It is then necessary to distinguish two cases:

- Windows Internal Private Network:

In this case, only Windows machines will be able to access the server with its host name.

Access from outside, especially internet, will only be possible if a VPN is set up.

If terminals that do not run on OS Windows (smartphones and tablets Android or iOS for example) must access the server, it will need to set up a DNS.

- External public network:

In this case, the web server must be on a public domain with a name assigned by a public DNS. This will allow web clients to access the server from an external network and whatever their OS (Android, iOS ...).

---

<sup>3</sup> DNS : Domain Name System

**TO REMEMBER**

## Domains and name resolutions

Access	Domain	Name resolutions	OS Client web compatibles
Private on internal network	Windows	Windows	Windows
		Private DNS	Windows, iOS, Android
Private on external network with VPN	Windows	Private DNS	Windows, Android, iOS
Public	Public	Public DNS	Windows, Android, iOS

The use of the IP address or machine name is incompatible with HTTPS certificates and will cause an alert message.

## 4. Examples of architectures

The architectures presented below are examples that cover different typical deployment scenarios. All architectures implement the HTTPS protocol - SSL / TLS and rely on the Microsoft IIS web server.

On the other hand, in the context of accessing web & mobile clients for a supervisory system it is important to distinguish the different roles as described below:

- A SCADA acquisition server acquires real-time data from equipment on a field network and supplies SCADA customers on an industrial network.
- A web server station hosts the web services and applications of the supervisor and is based on Microsoft IIS. The web server can be on the same machine as SCADA Web Back end or a separate one.
- A SCADA backend web station serves as a gateway to provide the data to the web server. The supervisor must be installed on the machine playing the role of web back end and the application must include the back end configuration. SCADA web back end may or may not be on the same machine as the web server.
- Web & mobile clients are remote terminals that access supervisor data either through an internet browser or a mobile application.

## 4.1 Architecture #1: Simplified « All-in-one » deployment

### 4.1.1 Description

The diagram below shows the case of a simple architecture in which the web server and the SCADA Web back-end are located on the same machine on an industrial network, on which the web and mobile clients are also connected.

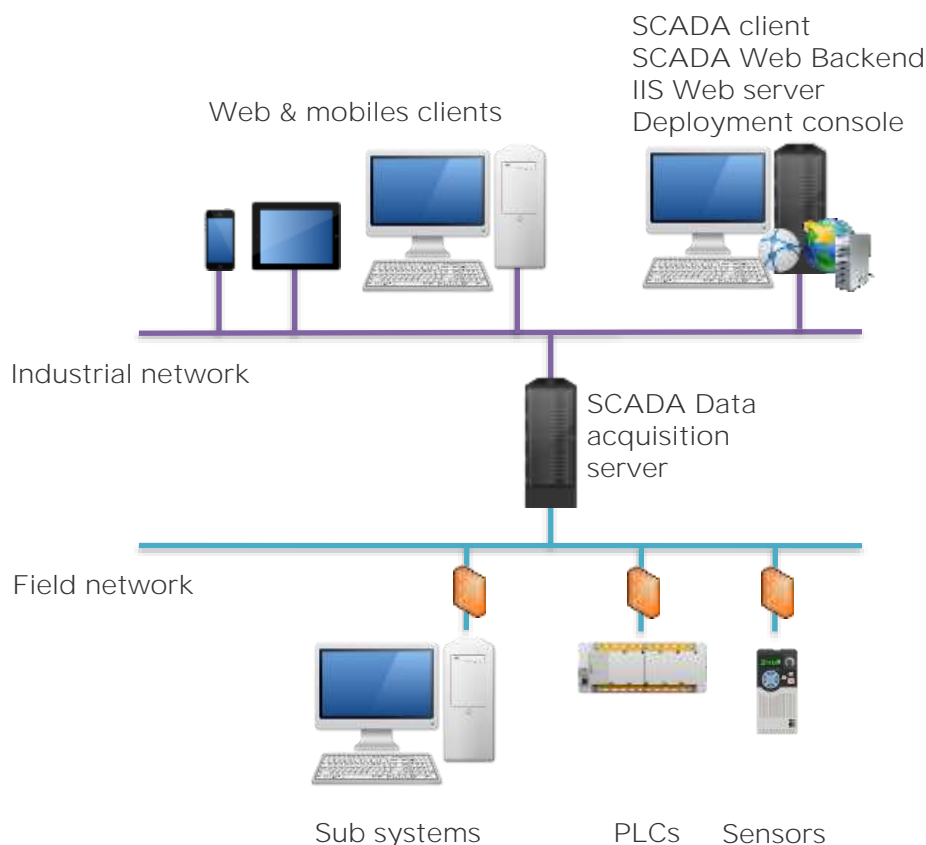


Figure 4 – Simplified architecture "All-in-one"

The use of a Windows server OS for the web server is not mandatory unless web & mobile clients are not running Windows OS and / or the expected number of connections is limited and the volume and load will not evolve in the future.

If non-Windows web and mobile clients are used the name resolution by a DNS server will be necessary, the one from Windows may be activated for example.

If a domain controller exists, it can be used to issue a security certificate, otherwise a "self-signed" certificate may be issued but will not be recognized as trusted and will cause an alert message.

Ideally, a deployment console will be installed on the web server to set up, deploy, and maintain deployment configurations.

In this type of architecture in which the networks are not segmented by routers and firewalls and the roles of each machine are not dissociated, the risk in the cyber security sense can be important if we do not take a few precautions use.

Indeed, the web server is the entry point for requests from web & mobile customers. If clients are on an outside network no protection exists to prevent reaching the acquisition server network and devices.

### 4.1.2 When to use this architecture

This architecture should be considered only if the network is private and completely isolated from outside access. Operators must not have access to administrative or internet networks, for example.

This architecture is irrelevant if the network must one day be open to the outside with user access from other networks.

In particular, this architecture is to be avoided if the access of web and mobile customers must be done from the internet and that there is no possibility of setting up a secure access solution such as a VPN.

It is therefore appropriate to reserve this type of architecture for limited needs in terms of deployment of web & mobile clients, on a closed network, with little or no evolution and managed by non-IT experts.

### 4.1.3 Benefits

The main advantage of such an architecture lies in the simplicity of implementation. Only one machine is needed to host the SCADA web server and web backend, and no network segmentation or flow control mechanism is implemented.

The configuration, deployment and maintenance of the web server are within the reach of non-IT experts especially if a deployment console is installed. This architecture allows low-security deployment scenarios, corresponding to limited needs such as the connection of few web or mobile clients, on Windows OS, in a private network and isolated from the outside.

TO REMEMBER

### Architecture #1: Simplified « All-in-one » deployment

- ✓ One machine performs all roles
- ✓ Non-segmented networks

Security level :  
LOW

Use :  
Private network deployment scenario completely isolated from the outside only

IT expertise required for deployment:  
LOW

## 4.2 Architecture #2: « All-in-one » deployment with internet access

### 4.2.1 Description

The scenario described here is often encountered on site due to the simplicity of its implementation. It nevertheless represents security risks that should be taken into account.

The architecture below shows a unique industrial private network on which there is a computer hosting the web server and the SCADA web back end as well as the SCADA acquisition server. The latter communicates with equipment connected to the same network.

Web & mobile clients access the web server:

- From terminals on the industrial network
- From terminals on an external network via internet box

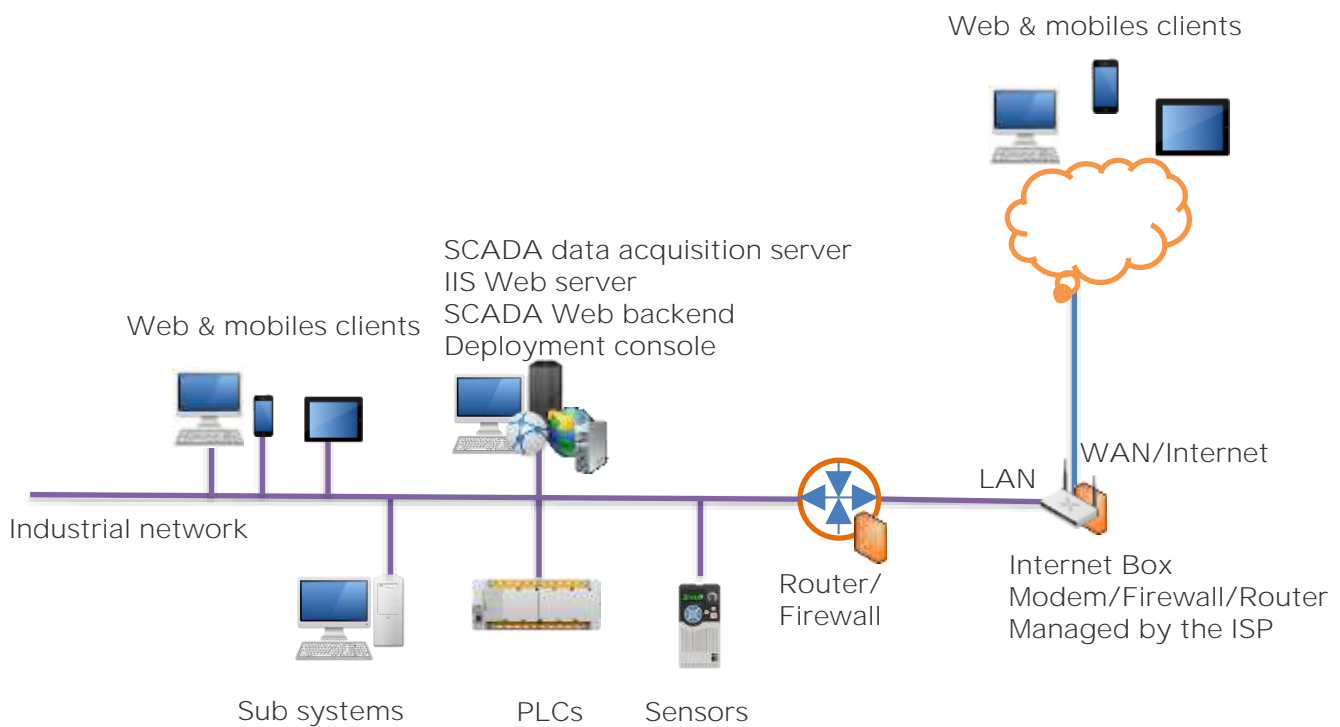


Figure 5 – « All-in-one » architecture internet access

The use of an internet box allows an implementation within the reach of all but also means that control and therefore trust (in the sense of cyber security) is delegated to a third party, the ISP<sup>4</sup> in this case. This represents a potential cyber risk for the related infrastructure and equipment. An update operated by the ISP on the box could lead to a

<sup>4</sup> ISP : Internet Services Provider

reconfiguration of data control filters for example and cause security breaches.

It is therefore strongly recommended to set up a device independent of the box for the routing and filtering of exchanges mastered by the infrastructure manager.

All stations and equipment are on the same network, there is no separation or segmentation of networks. In particular, the web server is not isolated, if a malicious request reaches him the network and connected equipment are directly exposed.

In order to validate the identity of the web server from less trusted networks and to avoid Man-in-the-Middle attacks - interception of exchanges between clients and the web server - the use of a certificate fully secure is essential. It can be issued through a trusted certification authority.

A deployment console will allow configuration and deployment of the elements necessary for setting up web and mobile clients.

## 4.2.2 When use this architecture

This deployment scenario allows access to web and mobile clients from an industrial network and from the Internet.

This kind of architecture, typical of old infrastructures or in transition to a deployment more in phase with the current security constraints, is not optimal in terms of security.

They should be avoided or reserved for cases requiring remote access and where there is no infrastructure managed by an IT team while being aware of possible risks for the facilities.



**TO REMEMBER**

## Architecture #2: “All-in-one” deployment with internet access

- ✓ One machine performs all roles within a single network
- ✓ Access from an unsecured external network

Security level :  
**LOW**

Use :  
Web & mobile client access from the internet

IT expertise required for deployment:  
Low to intermediate

## 4.3 Architecture #3 : Secure deployment by network segmentation and DMZ

### 4.3.1 Description

In this architecture, the external and internal networks are separated and on different security perimeters: the internal industrial network (LAN) is a secure private network, the external network (WAN) is a network of less trust, typically an administrative network or Internet.

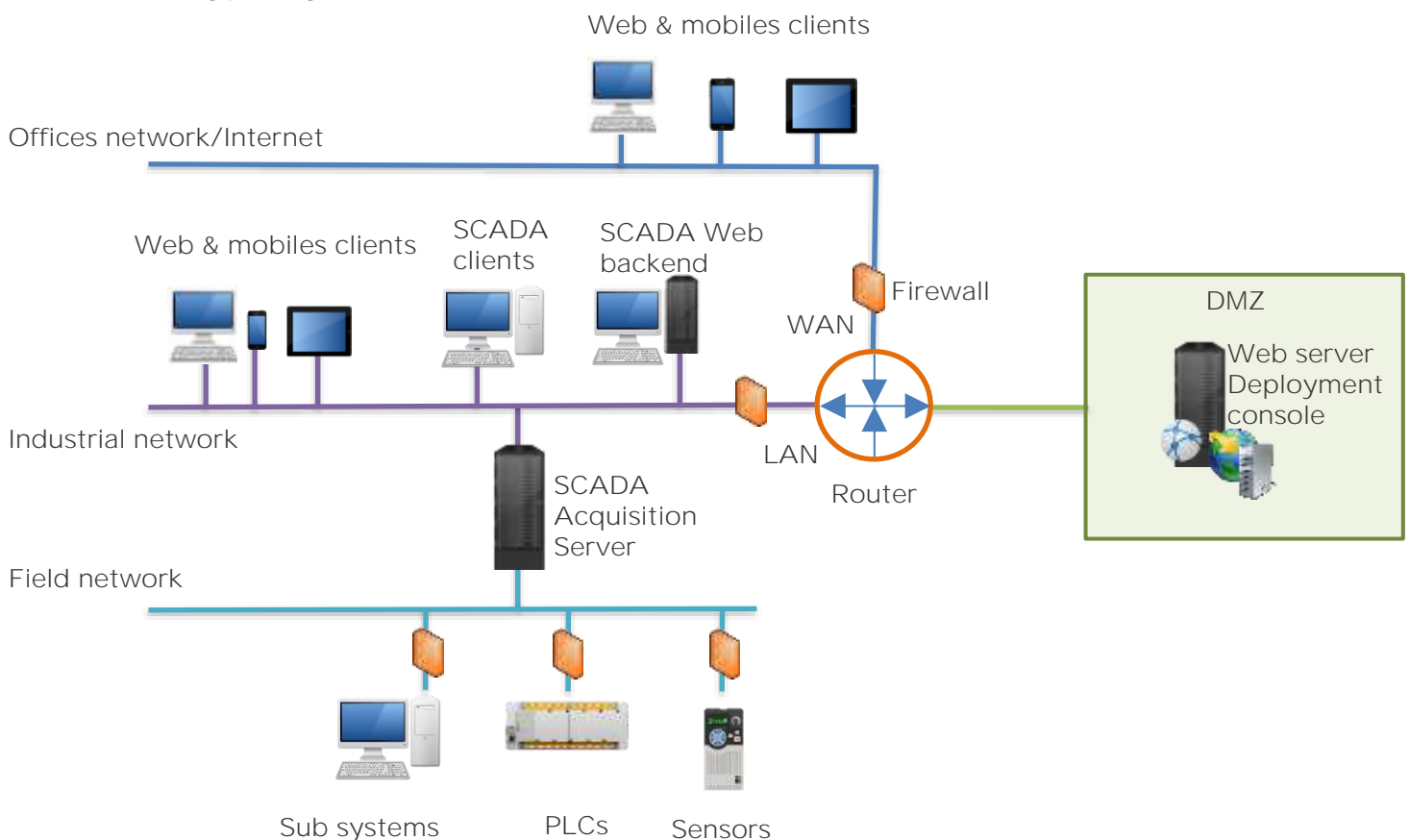


Figure 6 – Secure architecture by network segmentation and DMZ

The web server is hosted inside a DMZ and the SCADA web backend is hosted on a secure industrial network, both on a Windows server machine.

Web & mobile clients connect to the web server from the industrial network and from an external network.

In any case, the stations located on different networks can not have direct links with the other networks because of the segmentation by the router and the control of the firewalls.

In order to validate the identity of the web server from less trusted networks and to avoid Man-in-the-Middle attacks - interception of

exchanges between clients and the web server - the use of a certificate fully secure is essential.

This certificate can be issued:

- by the IT department if all Web and mobile clients are on a network administered by the same entity within the organization (eg Active Directory server of the corporate network).
- by the IT department via a trusted certificate authority if the web and mobile clients access the web server from an external network (standard access from the Internet by client computers / devices that do not have a trusted relationship with the client) network infrastructure of the company).

The resolution of the host names to access the web server is performed by a DNS server in the industrial network and a DNS on the external network.

A deployment console installed on the web server will be able to configure, deploy and make a complete diagnosis of the elements necessary for the proper functioning of the infrastructure supporting web & mobile clients.

### 4.3.2 When to use this architecture

This architecture is relevant when external access is needed and the load and number of web & mobile clients can be significant and evolve.

### 4.3.3 Benefits

This architecture allows access from less trusted networks in accordance with network separation practices with maximum control over network traffic, including the ability to block unwanted incoming connections from external networks to the industrial network.

This architecture provides the best deployment scenario in terms of security and allows maximum compliance with IT guidelines and practices.

**TO REMEMBER**

### Architecture #3: Secure deployment by networks segmentation and DMZ

- ✓ Web server station isolated in a DMZ
- ✓ SCADA backend Web station on an isolated and secure network
- ✓ Segmented networks, controlled flows

Security level :  
**HIGH**

Use :  
Web & mobile client access from outside trusted networks

IT expertise required for deployment:  
**Intermediate to high**

# TABLE OF FIGURES

---

Figure 1 – Industrial market shares 2019 .....	6
Figure 2 – Example of architecture with segmented networks .....	11
Figure 3 – Example of digital certificate.....	13
Figure 4 – Simplified architecture "All-in-one".....	19
Figure 5 – « All-in-one” architecture internet access.....	22
Figure 6 – Secure architecture by network segmentation and DMZ .....	25

Web & mobiles clients for supervision systems

Guide des bonnes pratiques de déploiement

Septembre 2019