UBIQUITY

UBIQUITY
The innovative remote assistance solution

UBIQUITY

In 2011 ASEM presented UBIQUITY, the innovative software platform for remote assistance and control.

The development idea came up to solve customer requests for an easy-to-use tool to install and setup machinery and, in particular, to manage post-sales service, phases during which customers often require modifications, customizations and support.

Traditionally, the most challenging aspect of meeting such needs is the availability of qualified technical resources, that would need the gift of **ubiquity**.

Designed for machine builders, the remote assistance and control solution UBIQUITY allows to operate on the remote system and its sub-networks as if it was in your own office.

UBIQUITY
Value added for all automation devices

The software solution UBIQUITY enables the access to remote supervision and control systems (based on Windows CE and Windows 32/64 operative systems) and to the automation devices (PLC, drive, etc) connected to the Ethernet and Serial sub-networks of the IPC/operator panel/controller/router, through a VPN (Virtual Private Network) based on proprietary technology optimized for industrial communication.

UBIQUITY does not require additional hardware and allows to operate in remote plants as if they were directly connected to your enterprise network. It enables technical support teams to solve any issue, eliminating the need for on-site assistance, dramatically reducing post-sale service costs.

This solution is particularly useful during machine setup and commissioning, to monitor remote applications, to modify and update software applications and remotely debug PLCs and other automation devices.

⊕ What I can do with UBIQUITY
→ Remotely program, debug and update IPC/operator panel/controller/router on which UBIQUITY runtime is installed
→ Remotely program, debug and update PLC and automation devices connected to Ethernet and Serial sub-networks of IPC/operator panel/controller/router on which UBIQUITY runtime is installed
→ Malfunction Analysis
→ Software applications updates

⊕ How it works
→ Uses a simple internet connection
→ Creates a VPN between the remote assistance PC and the remote device activating sub-network access
→ Activates safety procedures with end-to-end sessions without any intermediate
→ Ensures reliability and service continuity thanks to a redundant and distributed server infrastructure

⊕ Highlights

→ Remote control of the IPC/HMI/Controller/routers
→ Access to Ethernet and Serial devices connected to the IPC/HMI/controller/router sub-network
→ Additional tools: remote desktop, file transfer, chat, etc.
→ Proprietary VPN technology optimized for industrial communication
→ Available with the same features for Windows 32/64 and Windows CE platforms
→ No additional hardware required
→ SSL/TLS safe connection and use of certificates
→ Simple and easy-to-use interface
→ Distributed and redundant server infrastructure ensuring service continuity
→ Possibility to implement a private server infrastructure
→ SDK (Software Development Kit) for programming the activation of the Control Center functions also by external applications
→ Runtime with multiple connection support
→ Built-in firewall:
   - VPN communication protocols filter
   - Higher security and bandwidth control
→ Advanced user profiling and access control
→ Trace of all Domain administration activities
→ Trace of all session's activities
→ Internet sharing for LAN devices
→ Remote desktop via Web access
→ Automatic update of the runtime
→ Multimonitor remote desktop support
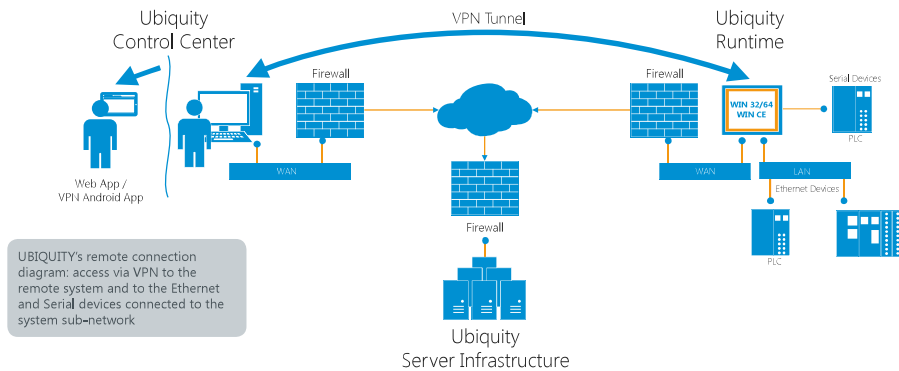→ IEC-62443-3 security certified
→ Support to NAT rules

UBIQUITY is a simple and ready-to-use solution. Its installation does not require any ICT expertise in network and firewalls configuration. It has a user-friendly interface that enables access to remote systems (PLCs, HMIs, drives, etc.) with a simple click through a VPN optimized for industrial communications.

The solution allows transparent management of remote systems as if they were connected to the enterprise network and it does not require the support of network administrators for any NAT, proxy, firewall, public IP and reserved ports.

UBIQUITY adds huge value in ASEM supervision and control system, but it is also a solution delivered as a software component to install on ASEM IPCs and third parties hardware.

UBIQUITY is included in all ASEM Windows based HMIs, PACs and IPCs.

UBIQUITY The components

Ubiquity
Control Center

VPN Tunnel

Ubiquity
Runtime

Firewall

Firewall

WIN 32/64
WIN CE

Serial Devices

PLC

Web App /
VPN Android App

WAN

WAN

LAN

Ethernet Devices

Firewall

PLC

Ubiquity
Server Infrastructure

UBIQUITY's remote connection diagram: access via VPN to the remote system and to the Ethernet and Serial devices connected to the system sub-network
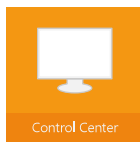
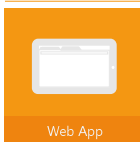UBIQUITY software platform is made of the following components:
→ The Control Center, the UBIQUITY VPN mobile App and the Web App www.ubiquityweb.net are the client applications that allow accessing the Ubiquity Domain and managing users, accessible devices and connections compatible with Windows 32/64 devices, Android devices
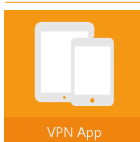
and any HTML5 compatible browser;
→ The Runtime available for Windows 32/64 and Windows CE operating systems installed on the devices on field, or integrated in the Ubiquity Routers;
→ The Server Infrastructure to implement the secure and fast end-to-end connection with the remote devices on field.
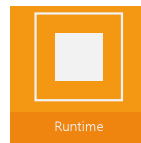
UBIQUITY Control Center
Control Center is installed and executed on the remote assistance PC and allows to manage the domain, the users and their privileges, and the connection with remote devices.
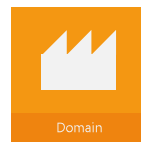
Control Center

Web App
The UBIQUITY web application allows, with a web browser, to access the desktop of the remote devices from PCs, tablets or smartphones.

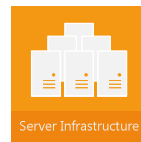**Web App**

UBIQUITY VPN Android App
UBIQUITY VPN Android App enables UBIQUITY VPN from Android devices to alla runtimes, routers and their subnet devices

VPN App

Runtime

UBIQUITY Runtime
The runtime is the software component installed and executed on the remote IPC/HMI/controller/router that supervises or controls the automation process. It requires neither additional hardware nor network configuration and it uses the existing Internet connection.

Domain

UBIQUITY Domain
UBIQUITY Domain is the "customer account" to make use of UBIQUITY infrastructure and services.

Server Infrastructure

UBIQUITY Server Infrastructure
Communication between Control Center and Runtime is ensured by a redundant server infrastructure built and maintained by ASEM which uses state-of-the-art security technologies for data exchange such as SSL/TLS, public key cryptography, safe, fault tolerant and redundant server farms to secure data privacy and adequacy.

Runtime versions
Runtime component is available in Basic and PRO versions for WinCE and WIN 32/64 operating systems. The Basic version provides access to the IPC/HMI/remote controller and provides remote-desktop, remote task manager, remote file manager and chat with the remote operator. The PRO version enables also the access to all the automation devices (PLCs, drives, etc.) connected to the Ethernet or Serial subnetwork of the remote IPC/HMI/controller/router . The Pro licence is available also as a portable licence, that can be moved up to 20 times to different devices.

UBIQUITY Runtime	Windows CE			Win32/64		
	Basic	Pro	Portable	Basic	Pro	Portable
Remote desktop (also multisession) file & task management, chat, screenshot	✓	✓	✓	✓	✓	✓
VPN to the remote device	✓	✓	✓	✓	✓	✓
VPN with access to the Ethernet sub-network of the remote system	-	✓	✓	-	✓	✓
VPN with access to the Serial sub-network of the remote system	-	✓	✓	-	✓	✓
Integrated firewall	✓	✓	✓	✓	✓	✓
API to interface proprietary software applications	✓	✓	✓	✓	✓	✓
Runtime operations persistent log	✓	✓	✓	✓	✓	✓
Multiple connections from different Control Center	✓	✓	✓	✓	✓	✓
Structured Domain creation, users and remote devices management	✓	✓	✓	✓	✓	✓
Internet connection via PROXY for Control Center and Runtime	✓	✓	✓	✓	✓	✓
Functioning in local network without license	✓	✓	✓	✓	✓	✓
Runtime update procedure with automatic shutdown and restart of services	✓	✓	✓	-	-	-
Log & Audit of Domain administration activities	✓	✓	✓	✓	✓	✓
Log & Audit of session's activities	✓	✓	✓	✓	✓	✓
Internet sharing for LAN devices	-	✓	✓	-	✓	✓
Movable up to 20 times	-	-	✓	-	-	✓
Automatic update of the runtime	✓	✓	✓	✓	✓	✓
Web access to the remote desktop	✓	✓	✓	✓	✓	✓
Multimonitor remote desktop support	-	-	-	✓	✓	✓

Domain types
UBIQUITY Domain is available in three different versions: Single Entity-Single Access, Single Entity-Multi Access and Multi Entity-Multi Access. Single Entity Domains are accessible by users of one only company, Multi Entity Domains are accessible by users of different companies. Single Access Domains give access to UBIQUITY infrastructure and services to one user at a time, Multi Access Domains give access to UBIQUITY infrastructure and services to more users at the same time.

	UBIQUITY Domain types		
	Single Entity-Single Access	Single Entity-Multi Access	Multi Entity-Multy Access
Domain accessible by	Users of one company	Users of one company	Users of more companies
Remote assistance services enabled for	One user per time	More users at the same time	More users at the same time

Server infrastructure

ASEM Server Infrastructure, for each customer related Domain, gives no limitation to the number of configurable users, devices, concurrent remote desktop and VPN sessions.

To provide an excellent service ASEM built a redundant and globally distributed server infrastructure that counts two farms in Europe (Munich and Amsterdam), two in the United States (western and eastern coast) one in South America (Brazil) and two in Asia (Singapore and Hong Kong).

Private Server Infrastructure

As ASEM provides a redundant and distributed Server infrastructure to manage UBIQUITY services,

it is also possible to replicate and build up a **private server infrastructure** managed autonomously.

Private Server
With the Private Server package, it is also possible to install a private server infrastructure in complete autonomy. The server application can be installed on dedicated systems or cloud servers.
Two types are available: Primary Server and Secondary Server.

The **Primary Server** is the basic software package and provides autentication security and communications as the ASEM server infrastructure.
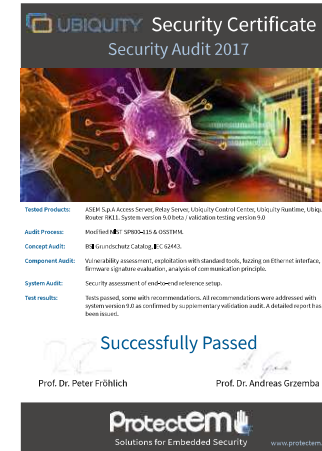
Primary Server:
→ Data storage: authentication, permission and security management
→ UBIQUITY Runtime licenses management
→ Relay feature to implement end-to-end communication

The **Secondary Server** is an optional package with relay functionality, to improve and increase the connectivity performances. It is possible to buy several secondary server licences and install them in different locations worlwide.

Secondary Server (option):
→ Relay feature to implement end-to-end communication
→ You can install multiple instances to reduce latency and balance traffic load.

UBIQUITY
Highlights

UBIQUITY Security Certificate — Security Audit 2017

Tested Products: ASEM S.p.A Access Server, Relay Server, Ubiquity Control Center, Ubiquity Runtime, Ubiquity Router RK11. System version 9.0 beta / validation testing version 9.0

Audit Process: Modified NIST SP800-115 & OSSTMM.

Concept Audit: BSI Grundschutz Catalog, IEC 62443.

Component Audit: Vulnerability assessment, exploitation with standard tools, fuzzing on Ethernet interface, firmware signature evaluation, analysis of communication principle.

System Audit: Security assessment of end-to-end reference setup.

Test results: Tests passed, some with recommendations. All recommendations were addressed with system version 9.0 as confirmed by supplementary validation audit. A detailed report has been issued.

Successfully Passed

Prof. Dr. Peter Fröhlich   Prof. Dr. Andreas Grzemba

ProtectEM
Solutions for Embedded Security   www.protectem.de

Security Certified
UBIQUITY obtained the security certification for internet-based industrial communications.
It has been certified in every component and confirms its full compatibility with the reference standards IEC 62443-3.

This certificate further confirms the value of UBIQUITY solution setting the highest security standard of the industry.
All versions are regularly certified.

Proprietary VPN
Differently from VPNs based on the IP layer, UBIQUITY VPN works on the data-link layer bringing concrete advantages:
→ Remote assistance PC becomes part of the remote host network using the same physical IP addresses

→ Remote assistant can use broadcast-based protocols
→ It is not necessary to configure the gateway of the remotely accessed devices. The remote assistant connection appears as a locally connected IP.

Remotation of Serial Communication
UBIQUITY installs a virtual serial port on the Control

Center PC. This virtual serial port can be mapped on a physical port of the remote device executing UBIQUITY

Runtime.
Benefits:
→ Possibility to carry out supervision and diagnostics tasks on remote serial devices.

Multi-client
UBIQUITY Runtime supports multiple concurrent connections from different supervisors both with interactive session (remote

desktop, file transfer, etc) and in VPN. Control Center can activate multiple interactive sessions with different devices and only one VPN connection to a remote device.

Benefits:
→ Maximum productivity due to the possibility to operate simultaneously on the same system.

Full compatibility with the existing firewalls
UBIQUITY Control Center and UBIQUITY Runtime connection are automatically configured

using outbound connections which are recognized as safe and therefore allowed by firewall policies.

Benefits:
→ No need to configure the end-user's firewall and network. Only an outbound connection is necessary.

→ UBIQUITY automatically uses enabled TCP and UDP protocols and can use HTTP, HTTPS or custom ports, ensuring compatibility with existing IT policies.

Industrial Security
UBIQUITY infrastructure uses the highest network security standards, such as:
→ **IEC-62443-3** security certified
→ SSL/TLS protocol via UDP or TCP

→ Two factors authentication with ASEM Authenticator App for iOS or Android
→ Asymmetric cryptography and **X509 certificates** for authentication sessions
→ Symmetric cryptography for data transimission

→ Message Authentication Codes (MAC) for data integrity.

UBIQUITY
Highlights

Integrated firewall

UBIQUITY's integrated firewall allows to control communication packets passing through the VPN. Introducing firewall policies, it is possible to filter Ethernet datagrams depending on communication protocols and target addresses.
The server infrastructure provides a library of policies that can be imported into the Domain and applied to devices and folders. Filtering rules can be assigned to single users or groups of users.
Benefits:
→ Increased security and bandwidth control
→ Increased flexibility in access permissions
→ Possibility to limit a user (or users group) to run only a certain number of software tools

Access profiling and control

UBIQUITY allows the creation of an unlimited number of users, user groups, device groups, each with different access rules.
Permissions can be flexibly configured for each user, up to the single device or folder. UBIQUITY provides 4 different user profiles: **Administration** enables folders and users management, **Device Installer** allows to add new devices in the Domain, **Network security** enables configuration and set up of

Firewall rules, **Remote access** allows to practice remote access sessions.
Benefits:
→ Users can implement their own organizational structure (made up of users, administrators, power-users, third parties, limited users, etc.) to reach in a flexible and controlled way all customers around the world
→ Access to remote devices is properly secured and restricted to the required personnel.

Internet connectivity sharing with LAN devices

Internet connectivity can be shared with specific devices of the LAN network:
Benefits:
→ Internet access from laptops of IP phones connected to the LAN network
→ Usage of UBIQUITY runtime services on LAN devices
→ Access to the web servers of LAN devices

Automatic updates

With UBIQUITY it is now immediate to get information about the availability of an update for UBIQUITY Runtimes and UBIQUITY Routers selecting which devices need to be updated and when.
Updates can be executed immediately or scheduled within a specified time interval.
The process runs in safe mode and without the need for any presence on the field.
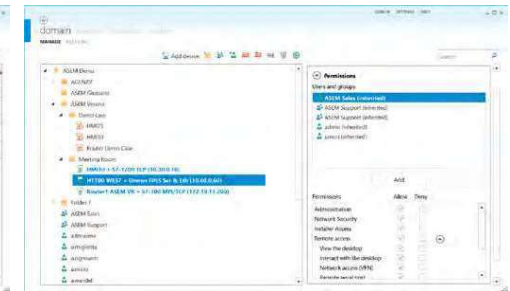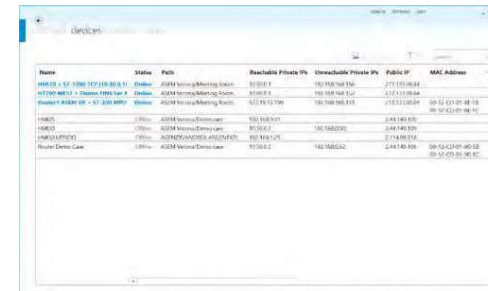In the same way, also UBIQUITY Control Center supports notification for updates availability, in order to keep it always aligned with the latest release.

Modern user interface

Control Center provides an intuitive graphic interface based on Modern-UI standards. The design presents additional controls and views, as the table view that enables the "Search" function using the text field on the right of the tree view that gives users (or groups of users) or device (directory) information.
Benefits:
→ UBIQUITY Control Center is easy, clear and intuitive
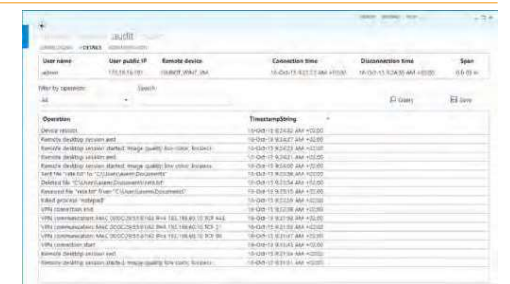→ Users' daily operations are simplified and immediate.

SDK Control Center

With the SDK (Software Development Kit) it is possibile to program the activation of Control Center functions also via external applications.
Control Center SDK is made of Assembly.NET components and a user manual for the usage of the API (Application Programming Interface) with the related code examples.
With the available interfaces you can execute the following tasks:
→ Domain login/logout
→ Browse domain
→ Connect/disconnect remote device
→ Connect/disconnect VPN
→ Connect/disconnect virtual serial port
→ File transfer to and from the remote device
→ Launch application on the remote device
→ End process and restart

Log and Audit of Domain and sessions' activities

→ Trace of all Domain Administration activities with a simple audit tool
→ Trace of all session activities: all activities and chat contents are registered for 30 days and accessible by domain administrators.

UBIQUITY
Highlights

Remote desktop
Control center includes a remote desktop function.
Benefits:
→ No need to activate RDP services or to install optional utilities like VNC.

File exchange
Control Center includes a complete tool to perform remote files download and upload.
Benefits:
→ No need to open shared folders or to install optional utilities like FTP servers.

Statistics and Audit
UBIQUITY records and stores all the remote access activities on the Domain.

Benefits:
→ The network administrator can verify anytime the post-sales support workload, the accuracy of the jobs carried out and get statistics for customers, PCs and operators.

Chat
Control Center and Runtime include a chat.
Benefits:
→ Instead of using the phone to communicate with remote operators, the user can simply take advantage of UBIQUITY chat reducing costs.

Cloud-based accessibility
UBIQUITY domain is registered on the Cloud. This architectural paradigm allows service continuity and data safety.
Benefits:
→ Wherever the user is located, he can launch Control Center getting access to remote machines worldwide.

Full support of Embedded platforms
UBIQUITY Runtime is available for the following operating systems:
→ Windows XP, Vista, 7, 8 (32 and 64 bit)
→ Windows Embedded Standard 2009, Windows Embedded Standard 7E and 7P
→ Windows CE 5.0, 6.0, Windows Embedded Compact 7.0

Connectivity quality measurement
UBIQUITY provides a simple function that measures connectivity quality on both local and remote network. Performances are measured in terms of latency time, jitter and packet drop.

Requirements

The following tables list the minimum hardware, software and network requirements for the correct installation and usage of UBIQUITY.

Control Center		
SW Requirements	**Operating System**	**HW Requirements**
.Net Framework 4.0 Client Profile	Windows XP SP3	At least Celeron 1.6 GHz with 512 MB RAM
	Windows 7 32/64 bit	
	Windows 8.1 32/64 bit	
	Windows 10	
	Windows Server 2008 and Server 2008 R2	
	Windows Server 2012 and Server 2012 R2	

Runtime		
SW Requirements	**Operating System**	**HW Requirements**
.Net Compact Framework 3.5	Windows CE 5.0 (x86)	256 MB RAM
	Windows CE 6.0 (x86)	At least CPU 500 MHz
	Windows CE Compact 7.0 (ARM, x86)	
.NET Framework 2.0 SP1 or 3.5 (distributed with setup)	Windows XP SP3	512 MB RAM
	Windows Embedded Standard 2009 (XPe)	At least CPU 500 MHz
	Windows Embedded Standard 7E/7P 32/64 bit	
	Windows 7 32/64 bit	
	Windows 8.1 32/64 bit	
	Windows 10, Windows 10 IoT Enterprise	
	Windows Server 2008 and Server 2008 R2	
	Windows Server 2012 and Server 2012 R2	

Private Servers			
Primary Server		**Secondary Server**	
Hosting	**Software**	**Hosting**	**Software**
2 public IP addresses, one of them associated to an Internet Domain name	Windows 7 64 bit or later	1 public IP address	Windows 7 64 bit or later
	Windows Server 2008 64 bit or later		Windows Server 2008 64 bit or later
	SQL Server 2012 or later, Express edition or greater		
	.NET Framework 4.6.1 Client		.NET Framework 4.6.1 Client