

SAVE

ANIE
AUTOMAZIONE



Utilization of mobile devices in SCADA systems

Leonetti Domenico

SIEMENS

Worldwide growth of smart connected devices



TRENDS

- ☐ Industry 4.0
- ☐ Smart Factory
- ☐ Internet of things
- ☐ Cloud
- ☐ Bring Your Own Device (BYOD)



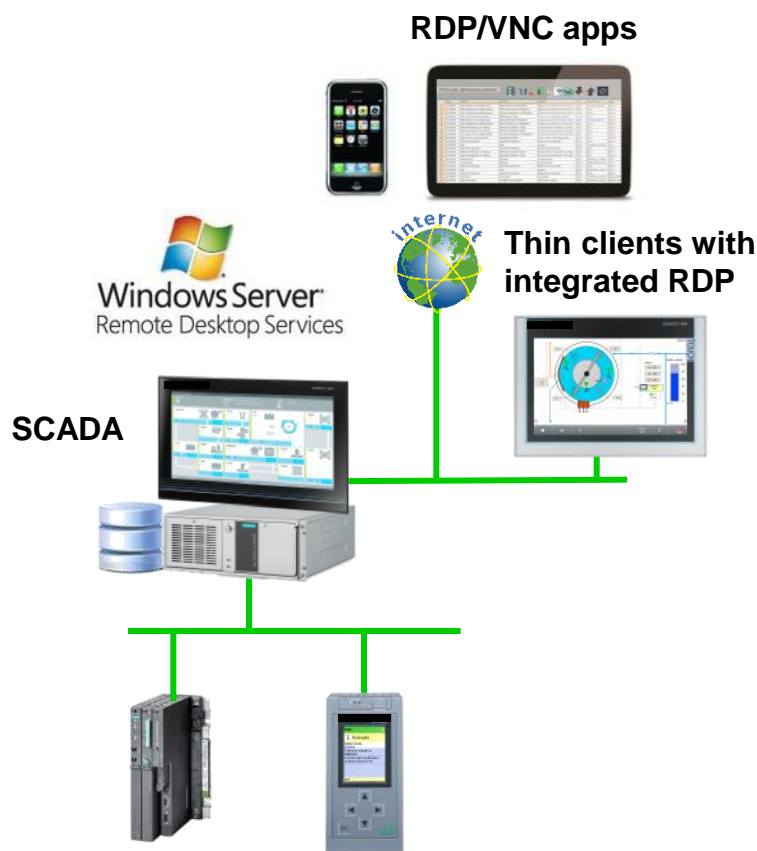
Product Category	2013 Unit Shipments	2013 Market Share	2017 Unit Shipments	2017 Market Share	2013–2017 Growth
Desktop PC	134.4	8.6%	123.11	5%	-8.4%
Portable PC	180.9	11.6%	196.6	8%	8.7%
Tablet	227.3	14.6%	406.8	16.5%	78.9%
Smartphone	1,013.2	65.1%	1,733.9	70.5%	71.1%
Total	1,556	100%	2,460.5	100%	58.1%

Source: Forrester Research, Inc. - 2013

Keys to success:

- Economic advantages (reduced TCO)
- Easy maintenance and lifecycle management
- Increase of productivity
- Commercial off-the-shelf (COTS) hardware

Utilization of “Thin Clients” connected via remote desktop to an existing SCADA system



Main features:

- Endurance to harsh environment (dust, vibrations, heat, water)
- Reduced Total cost of Ownership
- Increase of productivity (fast replacement)
- COTS hardware (commercial off-the-shelf) with integrated RDP client or RDP/VNC apps

Main issues:

- Limited number of remote desktop sessions (~25) running on the server
- Performances depending on the RDP/VNC connections and the number of clients
- Extra costs in the initial investment due to RDP CAL licenses on the terminal server

Pure Web Clients connected to an existing SCADA system configured as Web Server

Main features:

- Access via IP address from any browser based on HTML5 & SVG
- Independent from Web browser version (Zero Client side installation and no upgrades needed on device)
- Hardware platform independent (Windows, Android, Apple,..)
- SCADA information on WWW, LAN, WLAN
- No maintenance on the client device
- Monitoring and operation possible
- BYOD (bring your own device)

Main issues:

- Security
- Audit trail
- Migration and scalability of existing project



Security issues of plant remote control via Pure Web Clients

In order to avoid as much as possible unauthorized access to the SCADA server the following measures should be taken:

- Adopt a plant security policy
- Protect the WIFI connection with WPA2 secure password
- MAC address filtering
- Disable, if possible, USB and SD card interfaces
- Access via HyperText Transfer Protocol Secure (HTTPS) and SSL certificates
- Password rotation
- Training for operators to prevent social engineering attacks (good security habits, information security awareness...)

In some cases it makes sense to limit the use of handhelds to monitor only or adopt VPN as a single point of entry for a secure http traffic.



Extending SCADA features to mobile devices as an added value

The utilization of remote monitoring and control through mobile devices should coexist with the existing installations as an extra feature, guaranteeing continuity with the consolidated technology. This means:

- ✓ Migration from older versions of the SCADA system to the new web technologies possible, (saving the investment)
- ✓ Web publishing of the SCADA project with integrated tools
- ✓ No extra engineering or web technology required



The major players in the world of industry automation have already enriched their SCADA portfolio with new web options or apps for the main mobile app markets.



Some of them also offer dedicated industrial devices as Thin-Clients and industrial Tablet-PCs.

“Use cases” – focus on mobile devices as pure web clients



Management

- ✓ Monitoring production equipment from everywhere
- ✓ Better support for real-time decision
- ✓ Best informed anytime everywhere

Maintenance

- ✓ Mobile access to each equipment
- ✓ Simplified access even on wide distributed plants
- ✓ Faster reaction time to maintenance events

Reporting

- ✓ Access to the central information server on demand
- ✓ Automatic receiving of reports (KPI, production, assets)
- ✓ Facilitated manual data entry on site (e.g. quality lab)

Operator

- ✓ Monitoring the machines and production plant
- ✓ Take control for special use cases (audit trail advisable)

