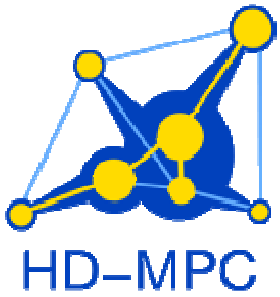
SEVENTH FRAMEWORK PROGRAMME
THEME – ICT
[Information and Communication Technologies]

Contract Number:	223854
Project Title:	Hierarchical and Distributed Model Predictive Control of Large-Scale Systems
Project Acronym:	HD-MPC



Deliverable Number:	D6.1.1
Deliverable Type:	Report
Contractual Date of Delivery:	March 1, 2010
Actual Date of Delivery:	**March 1, 2010**
Title of Deliverable:	**Report on results of hardware and software analysis**
Dissemination level:	Public
Workpackage contributing to the Deliverable:	WP6
WP Leader:	Universidad de Sevilla (USE)
Partners:	TUD, EDF, KUL, RWTH, USE, UNC, SUPELEC, INOCSA
Author(s):	D.R. Ramirez, M.A. Ridao, L. Sánchez

Table of Content

Project co-ordinator

Name: Bart De Schutter
Address: Delft Center for Systems and Control
Delft University of Technology
Mekelweg 2, 2628 Delft, The Netherlands
Phone Number: +31-15-2785113
Fax Number: +31-15-2786679
E-mail: b.deschutter@tudelft.nl

Project web site: http://www.ict-hd-mpc.eu

Executive Summary

This report shows the results of the analysis on hardware and software for hierarchical and distributed model predictive control (HD-MPC). The software and hardware needed to implement HD-MPC in industrial systems is almost the same as any industrial Distributed Control System (DCS). Also, HD-MPC techniques can be used in different applications, such as temperature control in large buildings, which require different technologies like sensor networks. Thus, this report is focused on the requirements, software, and hardware needed for industrial HD-MPC applications and also in those required in HD-MPC based on sensor networks.

On the industrial applications side, a number of commercial industrial control solutions have been considered (Invensys, Honeywell, ABB, Schneider-Telemecanique, Siemens and Telvent), which constitute a good sample of the whole offer. These systems are reviewed from the point of view of the requirements of a truly distributed control system. Thus, general, visualization and communications requirements and how each system can fulfill them are discussed. Concerning the communications requirements, the special redundant network topologies used in industrial DCS are reviewed and also the possibility of having different communication systems for those remote locations in which no other means of connecting to the net is available.

Another alternative to implement distributed MPC schemes is based on wireless sensor networks. Wireless sensors (often called motes) can have enough computing power to implement predictive control algorithms for typical industrial processes and also have very good networking capabilities. The advantages and challenges of designing wireless sensor networks for industrial applications are reviewed together with the main standards and operating systems used in those networks. Some hardware platforms are also reviewed.

The conclusions of this report is that truly distributed control systems must pay attention to a number of essential features that include homogeneous visualization systems, the possibility to extend the control system to all the levels of the business structure, a high degree of data availability, and a safe, redundant and easy to maintain network infrastructure. HD-MPC will do well on modern industrial DCS, as most of them offer open interfaces (like OPC) to access field data from third party software. Also, for some applications, HD-MPC can also be implemented over a mote network, provided that some modifications concerning the interface to industrial instrumentation are solved.

Introduction

This report shows the results of the analysis of hardware and software for hierarchical and distributed model predictive control (HD-MPC). Model Predictive Control techniques were focused from their beginning on industrial control applications, where their ability to handle multivariable processes and constraints has been very appreciated. The software and hardware needed to implement HD-MPC in industrial systems are almost the same as the ones used in any industrial Distributed Control System (DCS). HD-MPC techniques can also be used in different applications in other sectors, such as temperature control in large buildings, requiring different technologies like sensor networks. Thus, this report will be focused on software and hardware requirements needed for industrial HD-MPC applications and on those required in HD-MPC based on sensor networks.

On the industrial application side, a number of commercial industrial control solutions have been considered, which are a good sample of the existing commercial solutions. Among the largest and most ambitious platforms, systems from Invensys, Honeywell and ABB will be reviewed. These systems share a number of features like proprietary hardware for control and visualization, the ability to interface with third party hardware or even to integrate whole third party DCS into its own system. They have also been targeted as production control systems (Manufacturing Execution Systems, *MES*, or Enterprise Control System, *ECS*) whereas smaller systems are to be considered DCS for process control only. Furthermore, their network topologies are much more complex than those of the smaller systems. Among these smaller systems, some like the Siemens, Schneider-Telemecanique or Telvent ones will be reviewed. These systems have the classical structure of a DCS and have a scalable design that can evolve from smaller applications based on a unique personal computer to larger truly distributed control applications. Their network topologies can also be very simple or more complex but with simple and effective redundancy systems.

Traditionally some form of wired medium is used to connect sensors to the field control units and to computers. This is the best choice whenever possible and affordable. However, there are some situations in which a fully wired control system is not possible or cost effective. The number of sensors can be too large, they can be located at places unreachable by cable, or their mobility is required (e.g. as a mean of collecting data from a large space with few sensors). In these situations a wireless sensor can be better than a conventional wired one. Existing wired sensors can be retrofitted with wireless transducers to make them cable free, although they still use a virtual point to point connection to the field control unit. A more ambitious approach will be the use of purely wireless sensors (often called mote) that can be deployed to create a wireless sensor network in which every sensor module is composed of a microcontroller plus a wireless network interface. These wireless sensors will run a simple but effective operating system with real time characteristics and establish connections among themselves or with gateway devices that allow the exchange of information with control or corporate networks (see Figure 1). These wireless sensors must be cheap and energy efficient but with sufficient computing power and hardware flexibility. The network specification for an industrial wireless sensor network must have certain features like flexible and adaptive topology, self healing capabilities and different safety levels against intrusions and data theft. In this report, the requisites and features of industrial wireless sensor networks together with some representative hardware and software platforms are reviewed.

This document also analyzes different long distance communication systems. It is important for the HD-MPC Project to consider this type of communication system because some of the project application cases, such as the water capture system, the irrigation system or the hydropower valley, need long-distance communications.

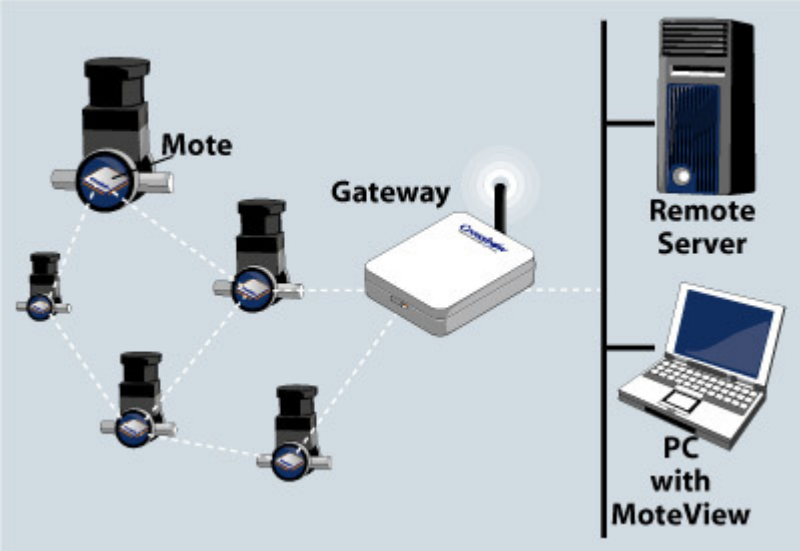


Figure 1

1 Industrial Control Systems for HD-MPC applications

In the following, some industrial control solutions will be reviewed. First of all, the main requirements for a truly distributed control application will be shown. These requirements have been grouped into general issues, visualization and communications requirements.

The first general requirement for a distributed control system is related to the global dimension of the system. The control system must be able to handle a large number of plants or process stations. Furthermore, for each plant or process, the system must be able to cope with a number of signals and variables that may also be large. Although remote stations are fairly autonomous, they usually have a control centre that must be able to integrate the information of the whole system, and also operate with any of the remote stations in real time. The DCS installed in the remote stations must not be the same in all of them. Because of the economical costs of having a unique control solution for all the remote stations, the system must be able to integrate with older or different DCS. Finally, a modern global distributed control system must be able to interface with an Enterprise Resource Planning (ERP) system like SAP ERP to be fully integrated in the industrial production structure.

Secondly, the requirements on visualizations for the centralized control center of a modern DCS are generally satisfied with a large video-wall or one or more large displays (like the one shown in Figure 2). These displays show as much information as possible with data

coming from any of the remote stations or system software packages. Although is not usual, remote operation of any of the stations from the central control center must be taken into account.

Figure 2

A very important group of requirements is related to safety in communications and interfaces provided for third party control software. The intranet of every remote station must be fault-tolerant with a balance in redundancy degree/economical costs. Different network topologies can be chosen, as will be reviewed later on in this report. Nowadays communications bandwidth is less an issue, but it should be possible to establish a priority in network access in function of the relevance of the data to be transmitted. It is very important for a modern DCS to be able to exchange data with other software in an easy and standard manner. Among the different protocols, modern DCS must support the most usual OPC interfaces (data access, events and alarms, historian and batch processes). This is very important in the planned HD-MPC applications, as no commercial DCS has such predictive controllers implemented as native or library components.

Besides the intranet communications, a truly distributed control system must have safe communications between each remote station and also with the centralized control center. Simple but unreliable and unsafe communications can be established over the Internet. Safety requirements demand more, and thus, Virtual Private Networks (VPN) can be considered. Through these networks, the DCS can exchange data and, also, other services like video or voice over IP can be used. The access to these networks can be made through standard networks connections, but often, in remote geographical locations, the use of a standard connection will be impossible or very expensive due to new cabling, etc… In these cases, alternate communication systems, as satellite links, must be used and the limited bandwidth of these links must be taken into account to establish priorities in network access.

Summing up, the main requirements for a modern DCS are shown in the following table:

General requirements	☑ Able to handle large systems with many remote stations each with many signals and variables and possibly heterogeneous DCS. ☑ Real time operation and data integration of all remote stations in a centralized control center ☑ ERP connectivity. ☑ Flexible and open system with support to standard protocols.
Visualization requirements	☑ Video-wall or several large displays. ☑ Able to show the remote stations process displays in the centralized control center. ☑ Able to operate any of the remote stations from the centralized control center with unified HMI.
Communications requirements	➢ Intranet requirements: ☑ Redundant network, ring or bus topologies. ☑ Priorities in bandwidth usage. ☑ Standard protocols: OPC. ➢ Requirements on the communications between stations: ☑ Able to transmit video from the stations. ☑ Voice channels (voice over IP). ☑ Safe Communications (VPN). ☑ Satellite links if needed.

Table 1

From all the available commercial systems, the followings will be considered:

- InFusion (INVENSYS).
- Experion (HONEY-WELL).
- System 800xA (ABB).
- Vijeo (SCHNEIDER – TELEMECANIQUE).
- WinCC (SIEMENS).
- OASyS DNA (Telvent).

The first three systems are the most ambitious in the number of functions and scope. InFusion is an ECS that it is closely coupled with Invensys DCS-only I/A series, but it is included here because it packs most of the advanced features of the Invensys control solution. Vijeo, WinCC and OASyS DNA are scalable and flexible systems that can be used for small to large systems but lack some of the features of the first three solutions.

In the following, all the systems will be reviewed considering the degree of fulfillment of each of the previous requirements.

1.1 General requirements

1.1.1 InFusion (INVENSYS)

Invensys has two separate groups of control solutions, namely DCS (Distributed Control System) solutions and ECS (Enterprise Control System) solutions. The DCS are I/A Series, which is targeted for medium and large plants, or A^2 Series, the latter focused on small installations or networks of geographically dispersed small stations. The ECS is named InFusion [1,2,3,4,5,6] and its main function is to integrate all the information of the DCS of the remote stations and distribute it along the enterprise structure, so that the visibility level between operation and business centers is increased. It is the responsible of computing production data in the form of Key Performance Indicators (KPI) that can be used to take decisions about production Schedule. The remote stations data is presented in real time. Supervision is possible as well as operation of the remote stations from the control center. All of these functions are focused on increasing production based on an unified collaborative environment.

One of the key points of InFusion is the asset optimization, extending feedback control from plant to business centers. Also, it can be integrated with standard software from Microsoft or SAP. This is possible because InFusion supports standard protocols like OPC or ODBC.

InFusion can work with DCS of Invensys as well as other brands. In most cases, the support for third party DCS is direct, but in the most difficult cases a custom gateway must be programmed to integrate all the DCS data in InFusion. Each remote station can have a different DCS, but InFusion will present the data of each station in a uniform way.

The InFusion architecture is shown in Figure 3. It is composed of a hierarchy of levels:

- Redundant and fault tolerant control network (connects field devices with DCS)
- Safe control information network (connects the DCS with other components of InFusion).
- Intra-Enterprise level network (Internet based network that connects InFusion with other departments and software of the enterprise).

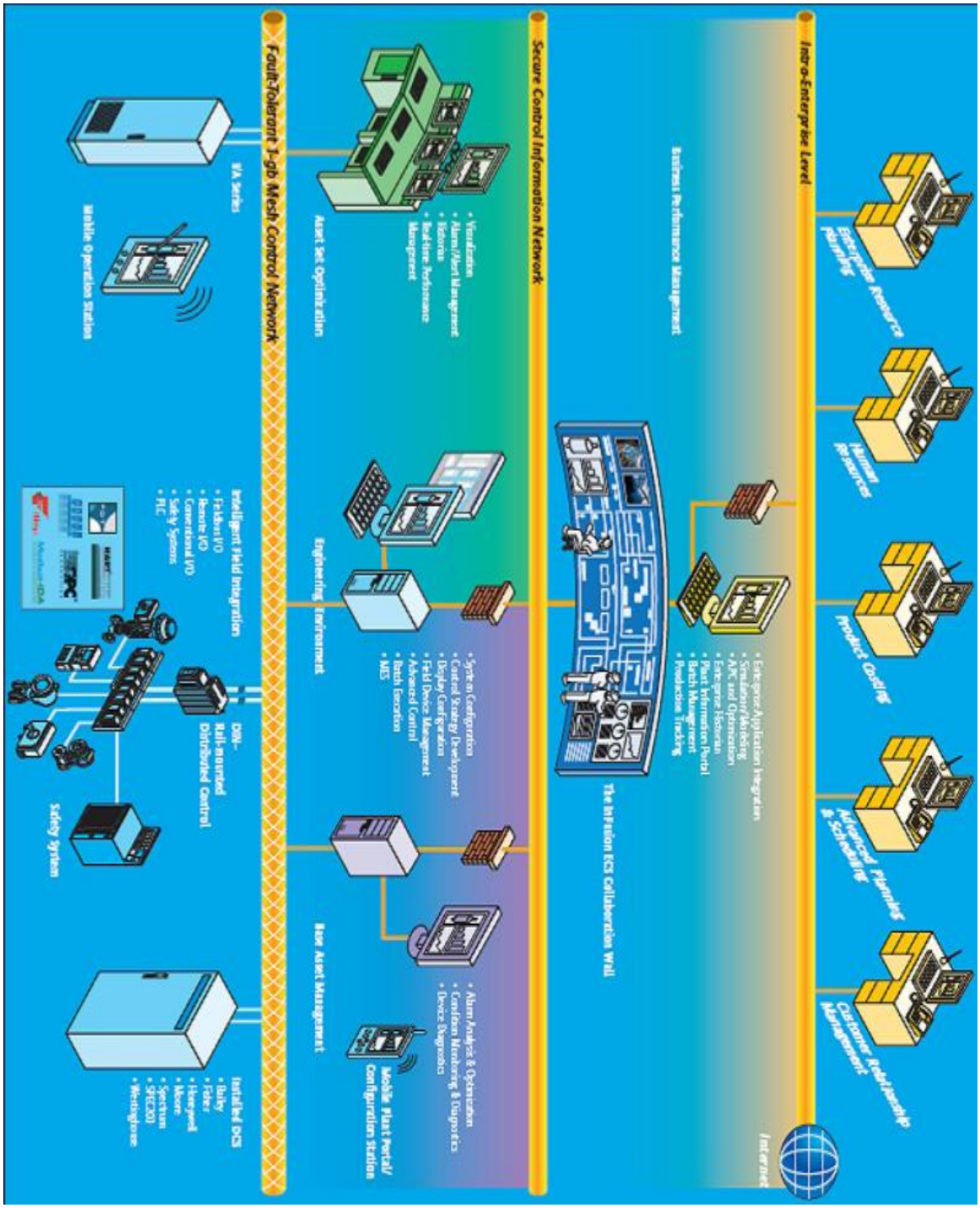

Intra-Enterprise Level
Enterprise Resource Planning
Maintenance Resources
Product Quality
Advanced Planning & Scheduling
Operations Reliability Management
Internet
Business Performance Management
Enterprise Application Integration
Simulation/Modeling
APC and Optimization
Enterprise Historian
Plant Information Portal
Batch Management
Production Tracking
The Infinium ECS Collaboration Web
Secure Control Information Network
Asset Set Optimization
Visualization
Alarm/Alert Management
Historian
Real-time Performance Management
Engineering Environment
System Configuration
Control Strategy Development
Display Configuration
Field Device Management
Advanced Control
Batch Execution
MES
Site Alert Management
Alarm Analysis & Optimization
Condition Monitoring & Diagnostics
Device Diagnostics
Mobile Plant Portal/ Configuration Station
Fault-Tolerant 1-gb Mesh Control Network
I/A Series
Mobile Operation Station
Intelligent Field Integration
FF-Ethernet I/O
Remote I/O
Conventional I/O
Safety Systems
PLC
DIN-Rail-mounted Distributed Control
Safety System
Installed DCS
Bailey
Fisher
Honeywell
Moore
Spectrum
SPECTRUM
Westinghouse

Figure 3

1.1.2 Experion PKS (HONEYWELL)

Experion PKS (Process Knowledge System) [7,8,9,10,11,12] is the control solution from Honeywell that integrates the functions of a traditional DCS and an ECS. All the software modules of Experion are designed following the principles of the ASM (Abnormal Situation Management) Consortium. Moreover, an auto-backup task is always running, so that a complete system can be recovered in less than an hour. Experion can work using proprietary real time units (angle mounted to maximize its lifetime, see Figure 4) or use third party units.

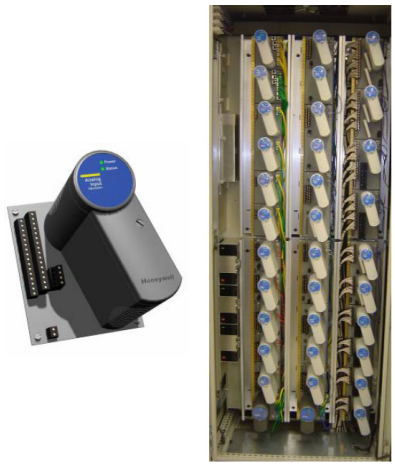


Figure 4

Experion design is based on well known industry standards like OPC, FOUNDATION™ fieldbus, HART, Profibus, DeviceNet, LON, ControlNet, and Interbus. It can also be integrated with SAP and other software like Microsoft Office.

Some distinctive features are the inclusion of a model based control package able to achieve better performance than the traditional PID controllers, and a complete simulation package that can simulate the control system itself (SIM-C200) as well as the plant to be controlled (Honeywell Shadow Plant). Experion also includes a specific video server that is used to supply real time plants video to the DCS.

Experion architecture can be considered a truly distributed system, in which a centralized control center is used to integrate the data of several remote servers each dedicated to a process. Communication between geographically dispersed plants is made over a wide area network (WAN) (see Figure 5).

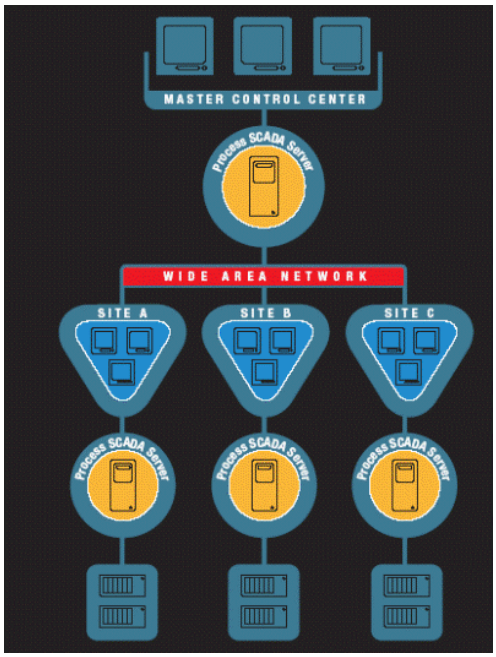


Figure 5

Experion architecture is also based on a hierarchy of levels each of them built around a network. These networks are:

- Local control network (LCN, for RTUs of system TDC3000).
- Supervisory control network (for new generation RTUs).
- Advanced control network (advanced controllers, video Server, simulation packages, etc…).
- Enterprise network.

Figure 6 shows Experion architecture as well as its main components.

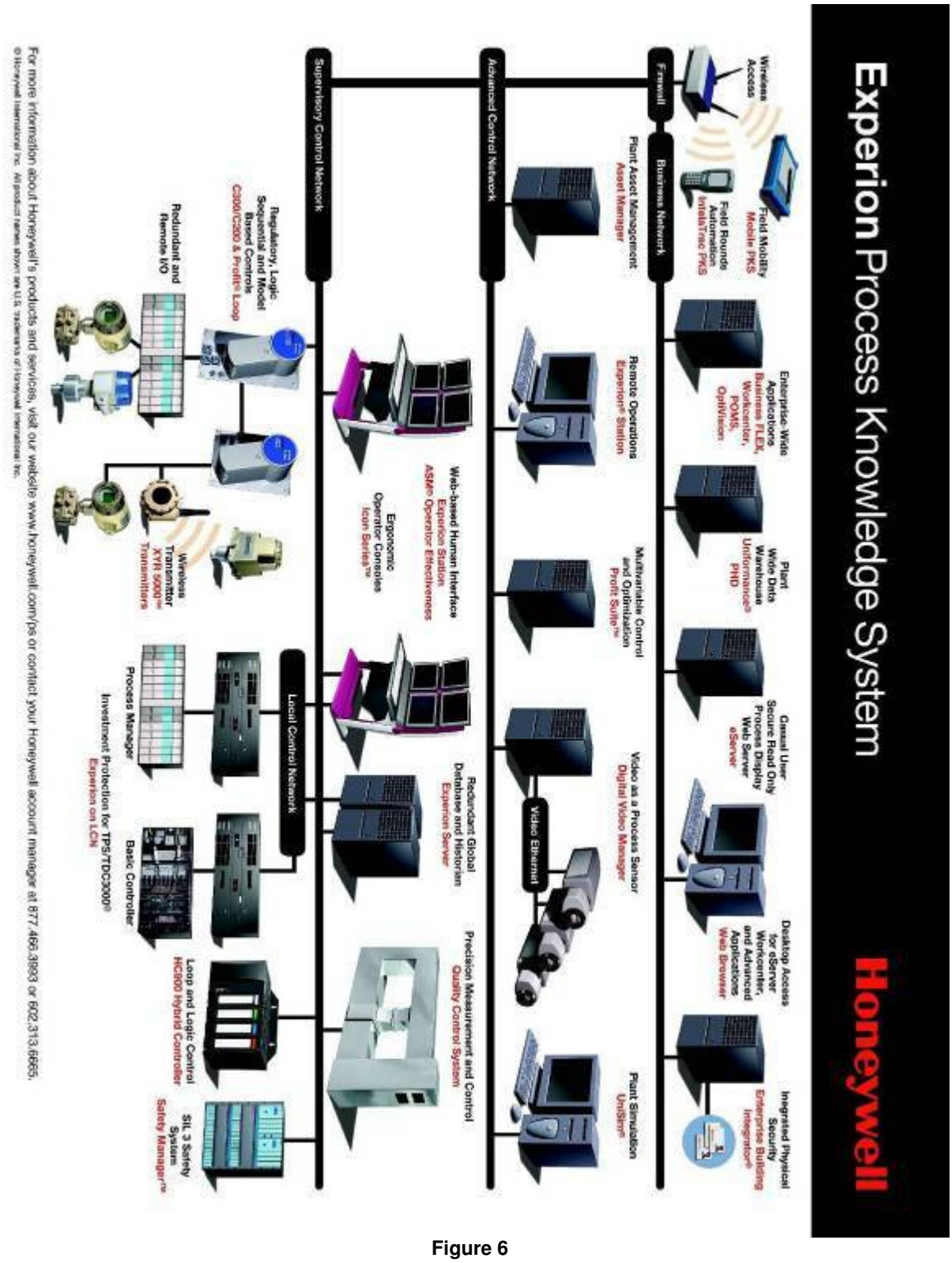

Experion Process Knowledge System
Honeywell
Wireless Access
Field Mobility
Mobile PKS
Field Rounds Automation
InfoTrac PKS
Firewall
Business Network
Plant Asset Management
Asset Manager
Enterprise-Wide Applications
Business FLEX, Workcenter, POMS, Optimizer
Plant Wide Data Warehouse
Uniformance PHD
Casual User Secure Read Only Process Display Web Server
eServer
Desktop Access for eServer Workcenter, and Advanced Applications Web Browser
Integrated Physical Security
Enterprise Building Integrator®
Advanced Control Network
Remote Operations
Experion® Station
Multivariable Control and Optimization
Profit Suite™
Video as a Process Sensor
Digital Video Manager
Video Ethernet
Plant Simulation
UniSim®
Supervisory Control Network
Regulatory, Logic, Sequential and Model Based Controls
C300/C200 & Profit® Loop
Redundant and Remote I/O
Web-based Human Interface
Experion Station
ASM® Operator Effectiveness
Ergonomic Operator Consoles
Icon Series™
Wireless Transmitter
XYR 5000™ Transmitters
Redundant Global Database and Historian
Experion Server
Precision Measurement and Control
Quality Control System
Local Control Network
Process Manager
Investment Protection for TPS/TDC3000®
Experion on LCN
Basic Controller
Loop and Logic Control
HC900 Hybrid Controller
SIL 3 Safety System
Safety Manager™
For more information about Honeywell's products and services, visit our website www.honeywell.com/ps or contact your Honeywell account manager at 877.466.3993 or 602.313.6665.
© Honeywell International Inc. All product names shown are U.S. trademarks of Honeywell International Inc.

Figure 6

1.1.3 System 800xA y ECS (ABB)

The DCS of ABB is named System 800xA [13,14,15,16,17]. It is a classical DCS without MES or ECS functions. Furthermore, ABB has its own MES called ECS (Enterprise Connectivity Solution), designed to work together with System 800xA. ECS provides integration with SAP and other ERP, as well as office applications. ECS has real time access to plant data and plant databases through OPC connections. ECS is designed to integrate with System 800xA, but it can also integrate with third party DCS (see Figure 7 and Figure 8).

System 800xA is a classic distributed control system which can perform most of the typical functions of these systems, such as:

- Control and management of field devices.
- Visualization

.

But also some other functions that can be performed by a MES:

- Production management / Asset optimization.
- Decision support.

System 800xA is designed to be used with ABB proprietary control hardware (Series 800 or Series 900), but can also be used with third party hardware as it has been designed to provide support to well known standard protocols like Profibus, Fieldbus or HART.

ABB's System 800xA architecture is rather less complex than Invensys or Honeywell solutions architectures, as it is a standalone DCS based on a safe control network which servers and RTUs are connected to. RTUs, in turn, are connected with field buses to control devices. The control network can also be connected to a WAN using a gateway to provide remote access using secure communication protocols. System 800xA architecture is shown in Figure 9.

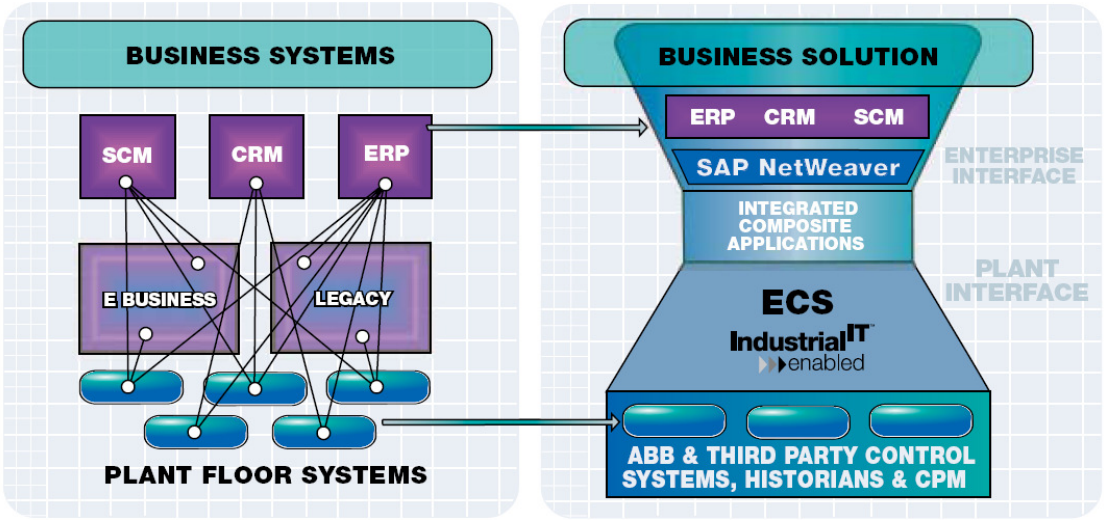


Figure 7

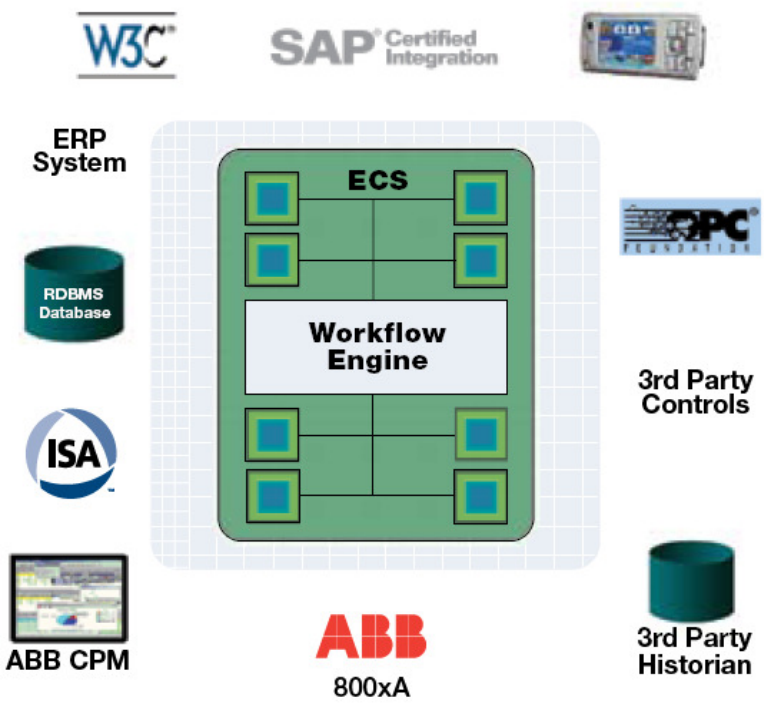


Figure 8

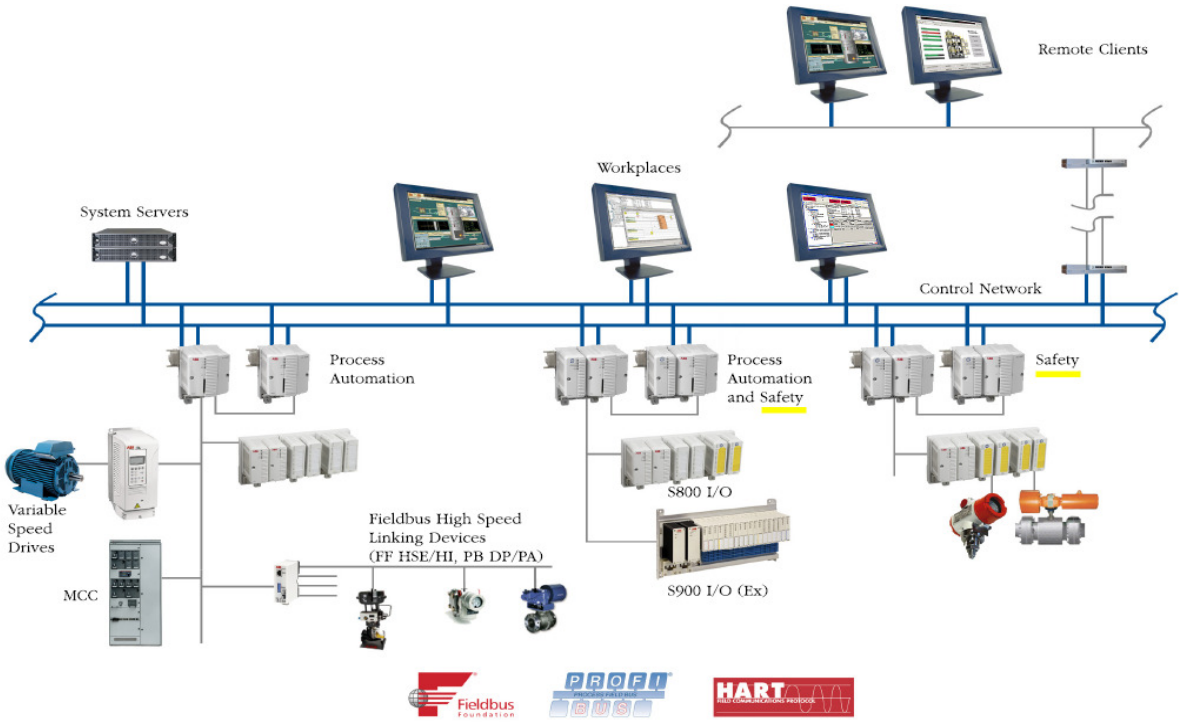


Figure 9

1.1.4 Vijeo (SCHNEIDER-TELEMECANIQUE)

Vijeo [18,19,20] is a DCS focused on small and medium applications but with a strong emphasis on scalability which allows its implementation in large systems. The main components are:

- VIJEO CITECT: SCADA with a limited report generation capability.
- VIJEO HISTORIAN: Module used to report generation from data taken from VIJEO CITECT. It is based on Microsoft SQL SERVER and has an interface to access ORACLE databases.
- AMPLA and META: Applications for MES functions and computing corporate indexes (KPI).

The Vijeo architecture is a client-server type. The scalability of the system means that a small installation can be made with just a computer and a Vijeo license, acting as client and server at the same time. This is very appropriate when just a RTU is required (see Figure 10), or several RTUs but with just one server and several clients connected to it through a LAN (Figure 11). For larger installations, the architecture can be more complex with clusters of servers that can be connected to clients through a WAN (see Figure 12). The scalability also means that one can start with a small installation of Vijeo CITECT and later on, if needed, evolve to a more complex configuration.

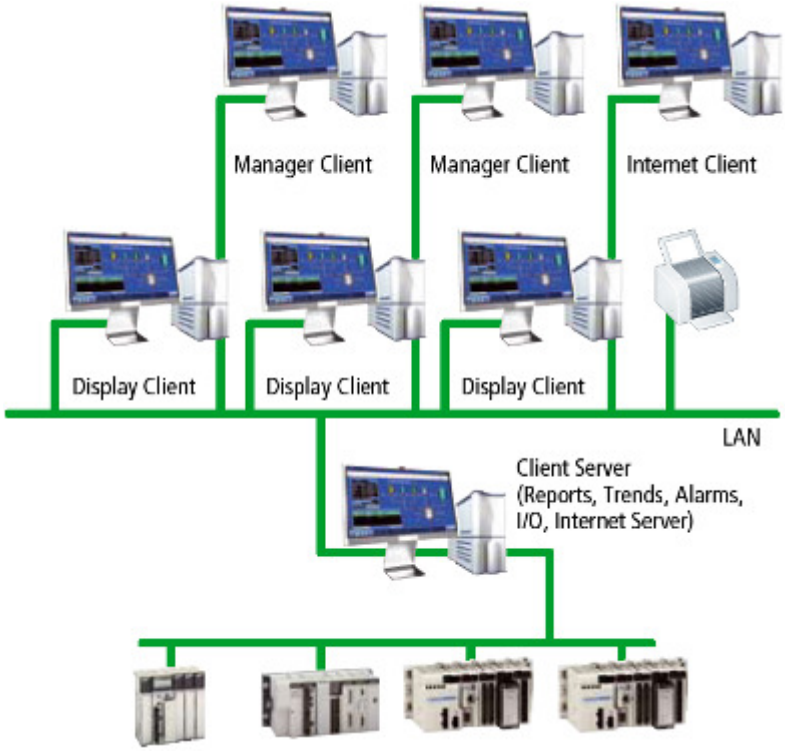


Figure 10

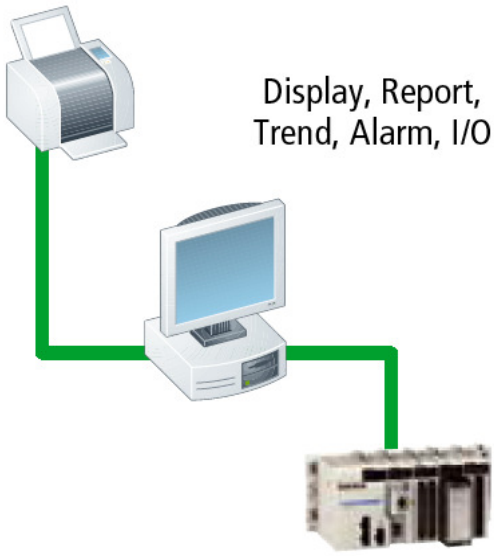


Figure 11

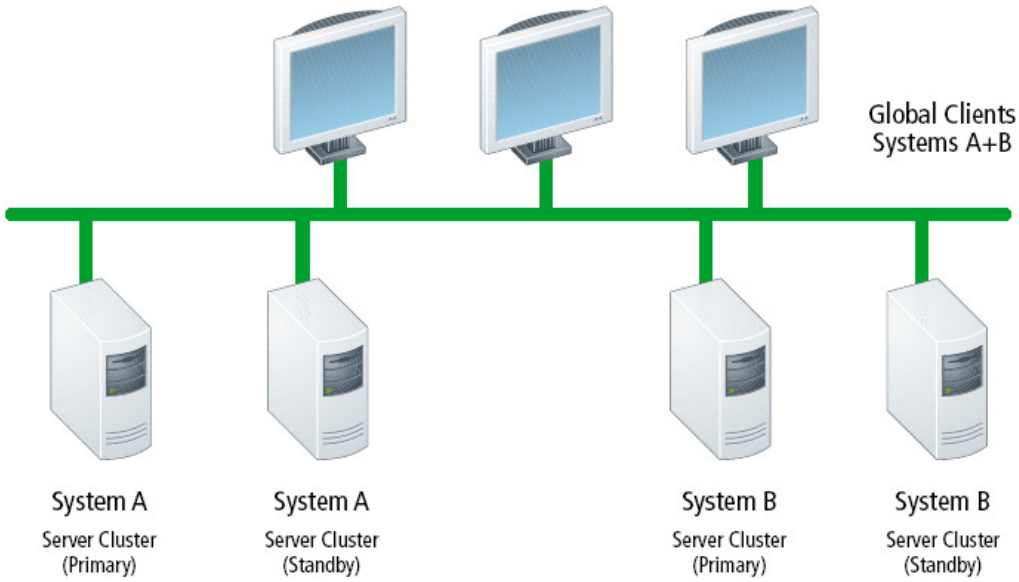


Figure 12

The client-application means that there are different servers associated to different tasks. These servers can communicate with other servers or clients. There are servers for real time data, alarms, trends and reports (See Figure 13). There a basically two types of clients:

- Display client: can monitor (read) and actuate (write) over a plant.
- Manager client: can monitor only.

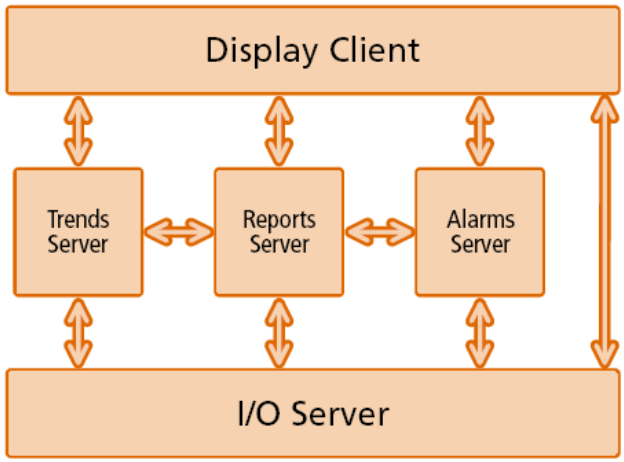


Figure 13

The flexibility of Vijeo architecture is evident when some processes are repeated in an installation. If this is the case, it is possible to configure a server for a process and replicate it for the remaining processes. The clients will be able to access to one particular server or to all of them at the same time (Figure 14).

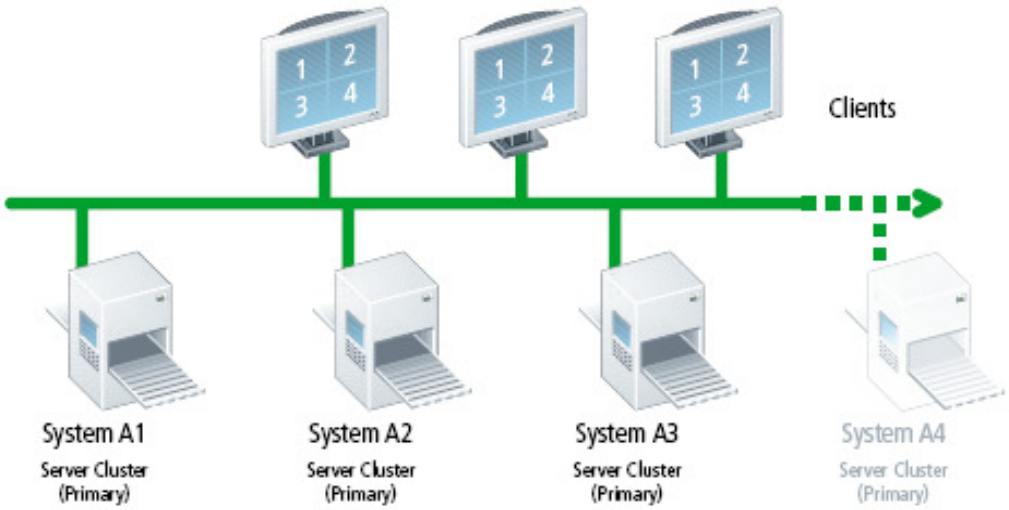


Figure 14

Other distinctive feature of Vijeo is the floating license scheme. This means that server or clients offline do not need a license. The only restriction is that the number of online servers or clients must match the number of licenses. This is very convenient when some servers are kept in standby as backup. Finally, Vijeo scripts can be programmed in its own proprietary language called CICODE or in Citect VBA (Visual Basic for Applications).

1.1.5 Siemens WinCC

WinCC [21,22] is a classical SCADA well known in engineering schools and focused to small and medium applications. The number of supported points is enough for these applications (up to 64000) but the number of supported servers (either online or backup) is limited to 12. The total number of clients is also limited to 32.

Access to data in WinCC is quite flexible, and, as in many other modern SCADAs, there is a web navigator, thin clients for accessing from PDAs and the "Data Monitor" which allows historian access from Internet Explorer or Microsoft Excel. These modules are included in a client-server distributed architecture which is illustrated in Figure 15.

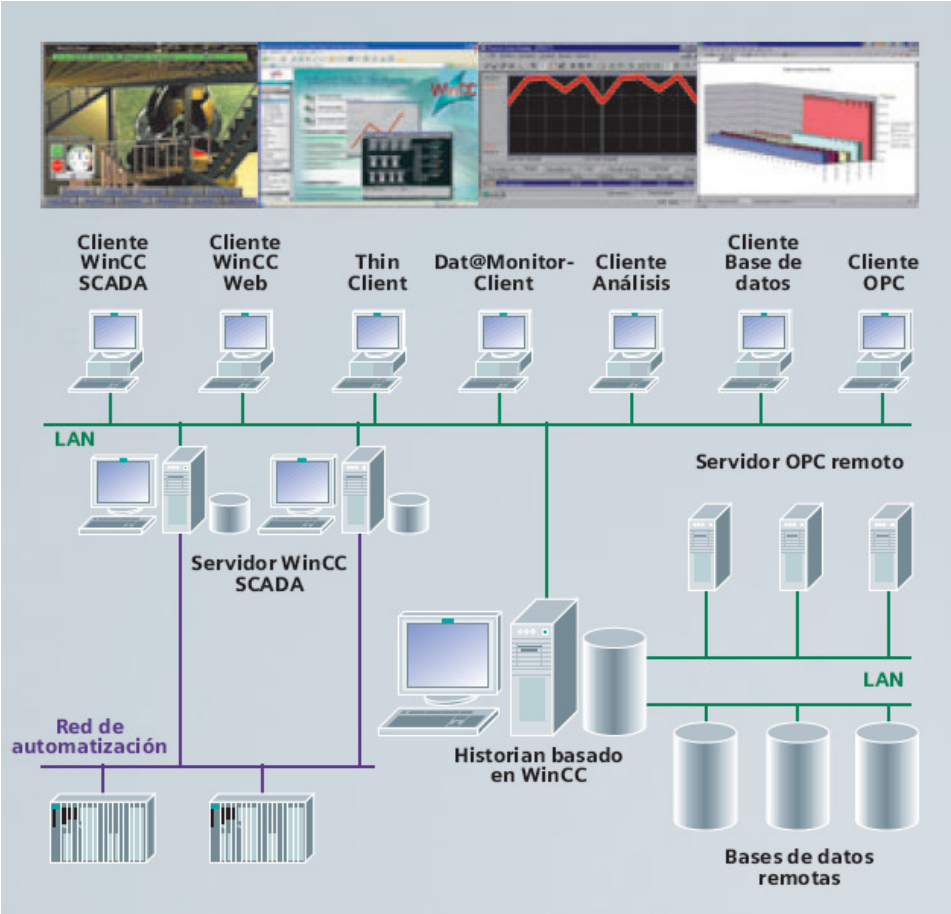


Figure 15

One of the WinCC modules, "Industrial Data Bridge", supports connections with other software packages (like MS Office) using OLE-DB and OPC-DA. An additional package, named "Connectivity Pack", allows the integration of WinCC with Enterprise management software like SAP-ERP using OPC interfaces. OPC also allows the interface of WinCC with MES systems (see Figure 16).

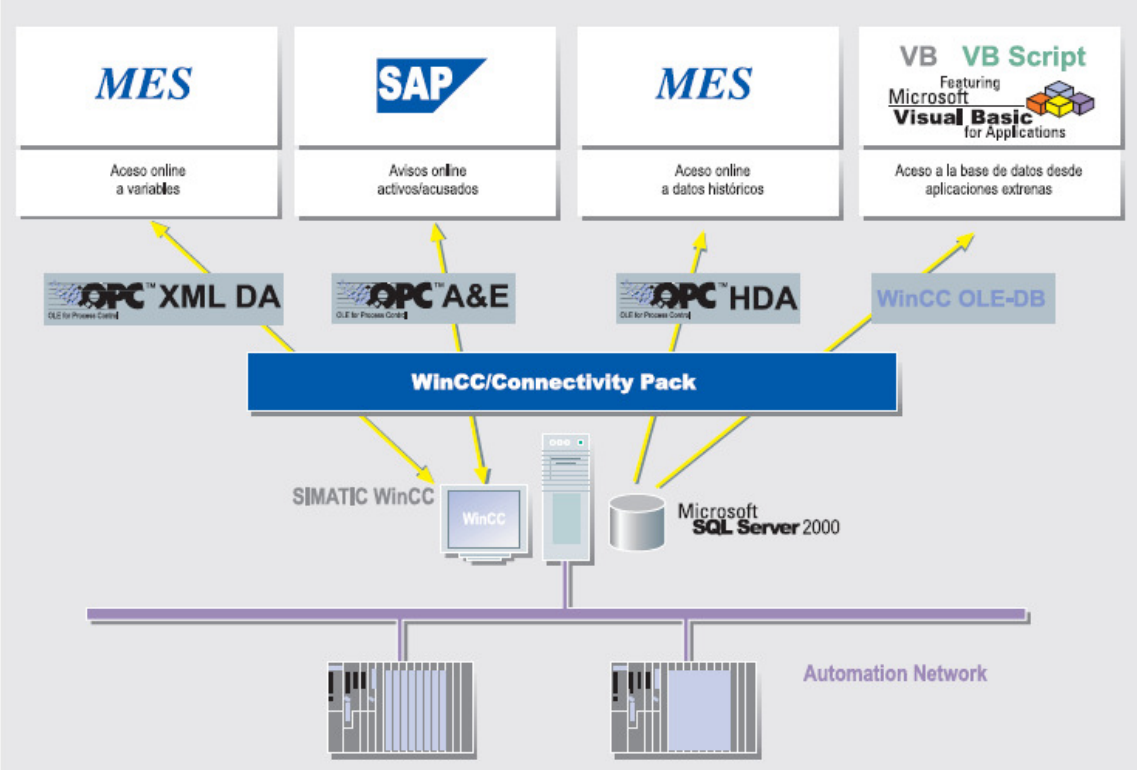


Figure 16

Other software modules or features included in WinCC are:

- WinBDE: computes production indexes (KPI), with production increment and shutdown events reduction as goals.
- Redundancy: availability is increased through redundancy
- ProAgent: failure and error diagnostics integrated in STEP 7 and S7.
- Audit: tracks every operator action and changes in the system.
- Totally Integrated Automation: everything is integrated in WinCC, like configuration and diagnostic of PLCs.
- Scripts can be programmed in Visual Basic or ANSI C.

1.1.6 OASyS DNA

OASyS DNA is a SCADA from Telvent, and like its name suggests, it is a Dynamic Network of Applications (DNA). This means that modules can be added, removed or updated in real time, reducing data duplication and exchanging data in real time.

The main components are the graphic interface (XOS), the relational database management system and the ability to integrate with third party applications. The purpose is to extend real time data access from the plant to the other departments. Connectivity is guaranteed

through the use of software standards: ODBC, OPC, SQL, SOAP, etc… This allows the exchange of data with MS Office, Lotus, SAP, Oracle, MS SQL, etc…

Since OASyS is based on network applications, its architecture, named DistribuSys, is purely distributed. Some of their features are:

- Field devices from a DCS can be controlled from other system.
- Backup systems can be defined for different DCS.
- Real time data can be shared among different DCS

The logic architecture of the system\ is composed of n levels, separating the human-machine interface, the logic used to present data (enterprise logic) and the data itself. There can be more levels associated to the enterprise level logic. Each of these levels can work, if necessary, in a different platform and can be updated and operated in an independent way. This also improves the scalability of the system. Figure 17 shows the OASyS architecture.

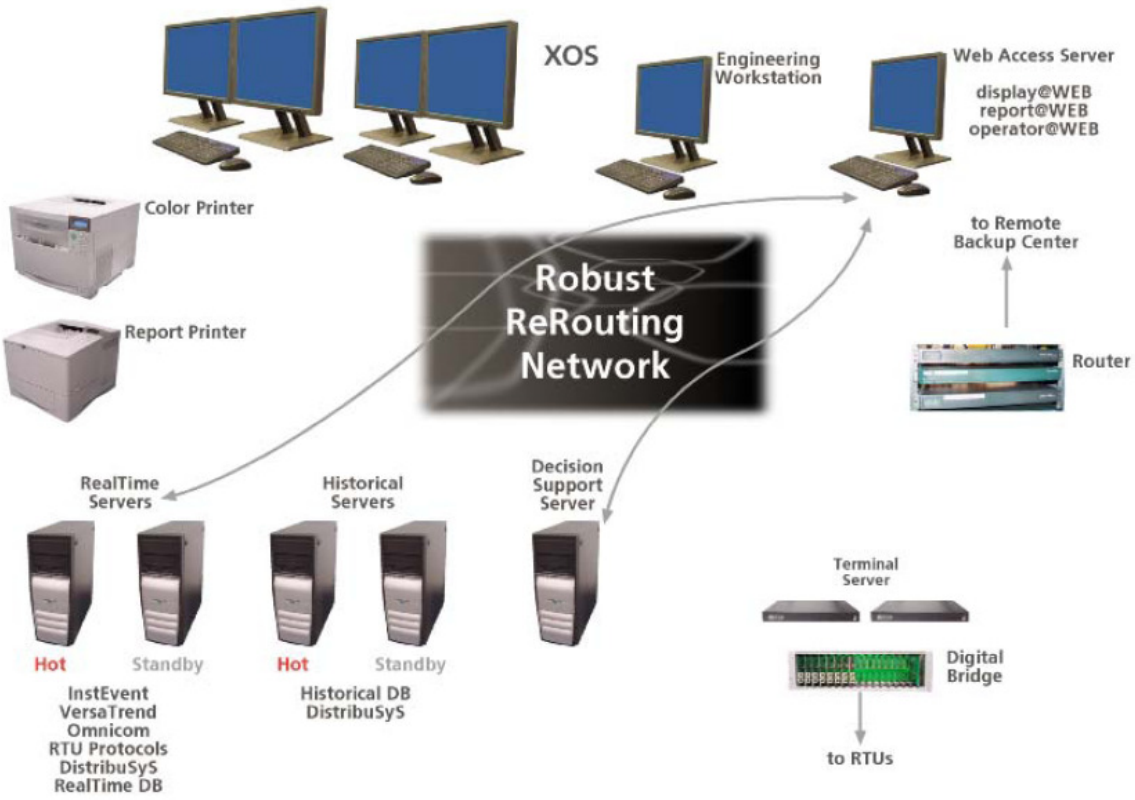


Figure 17

1.2 Visualization requirements

1.2.1 Invensys

The visualization scheme of Invensys Infusion is built upon two main components: the Collaboration Wall and the Infusion View [3].

The Collaboration Wall is a 3 meter display (see Figure 18) where specific user presentations can be projected. Moreover, the projected screen can also be displayed on conventional monitors and PDA devices. Everything that appears on the Collaboration Wall can be recorded, annotated and shared by all clients in the system. The latter feature is focused on transforming process graphics into a collaborative environment.

Figure 18

The Infusion View (see Figure 19), offers the typical options and features that can be found in any other SCADA (although Infusion is a MES, i.e. more than just a SCADA). Some of these features are:

- Hierarchical navigation, each system view can be expanded into a detailed view of each one of its subsystems.
- Components and alarm libraries.
- Real time data, historians and transactional data can be displayed in any device.
- InFusion View Terminal: thin client for PDAs, Tablet PC or bandwidth limited Web browsers.
- InFusion System Manager: Shows the status of field devices and networks.

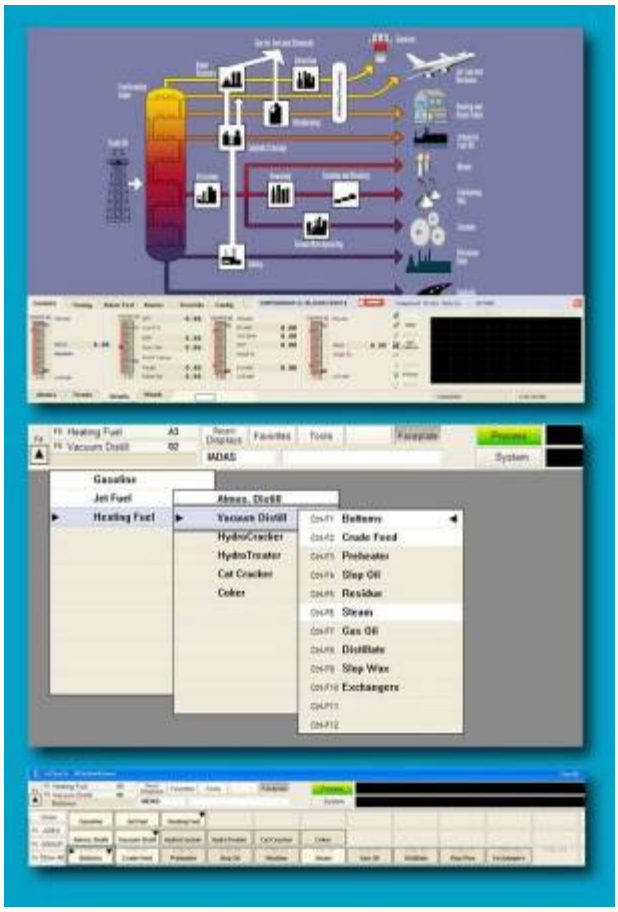


Figure 19

1.2.2 Honeywell

The visualization and interaction with Experion is mostly made through the Experion Station (see Figure 20). Console (ES-C) is the main control console and can be extended using Experion Station. Console Extension (ES-CE) allows up to 4 work spaces in the same console. Furthermore, the Experion Station-Flex (ES-F) client application can be used from any computer that has access to the server.

HMIWeb is Honeywell's technology used to provide HMI access from a web browser. It is based on HTML (ActiveX, with optional integrated video) and it is used in the software of Experion Station and also with Internet Explorer. Event and alarm presentation follow normalized formats (ASM and EEMUA).

Obviously, Experion Station includes all typical features, some of them can be highlighted:

- Hierarchical navigation.
- Integration of events originating in external OPC servers.
- Report generation:
  - Alarms/events.
  - Tag point attributes (invalid values, etc…).
  - Event sequences.
  - Formats compatible with Microsoft Excel, CSV and free format.

- eServer (see Figure 21and Figure 22) to allow safe casual access:
  - Internet Explorer can be used to access process graphics, etc…. from outside the system.
  - Works with Windows CE.

Premium version also allows access from Internet Explorer to more advanced features such as trend graphics, report generation, etc…

Figure 20

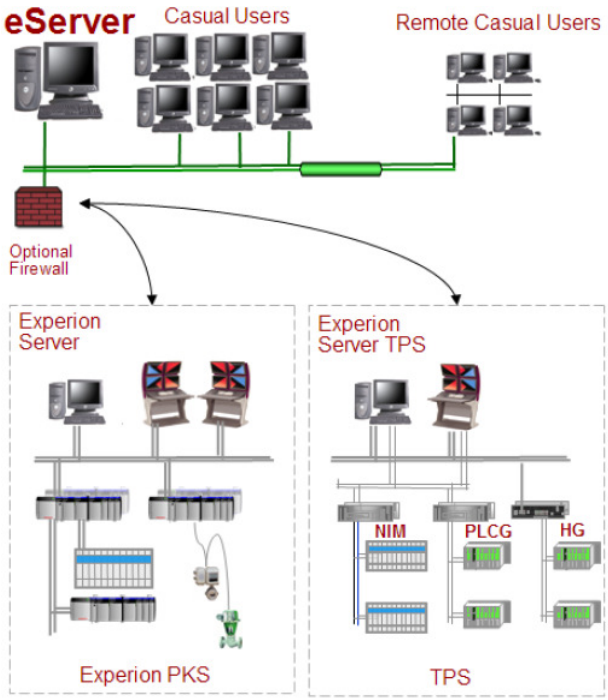


Figure 21

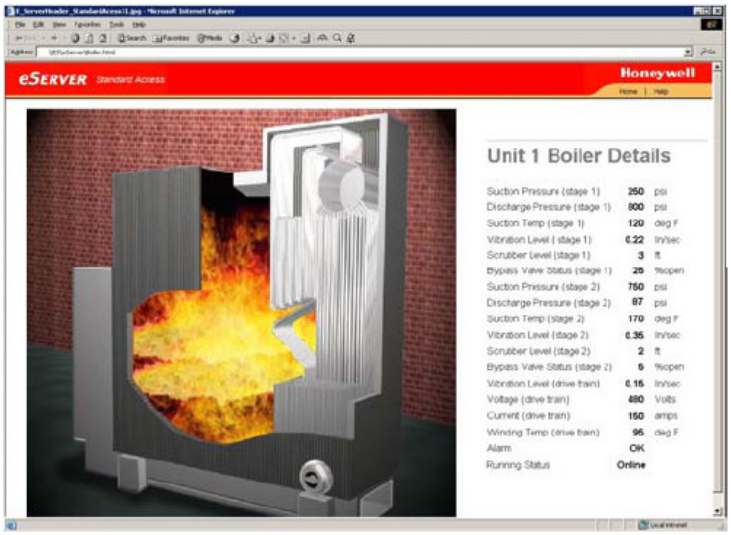


Figure 22

1.2.3 ABB

The visualization module of ABB, is the Process Portal. Navigation is intuitive and presentation and report generation is tailored to each specific user. Thus, each presentation has alarm and process displays as well as menus customized to each user. Moreover, security levels can be assigned to each user, so that it is possible to define what can be displayed and where it can be accessed from. Figure 23 shows an example of a typical business user view, Figure 24 shows a maintenance view, and Figure 25 shows the typical operator display.

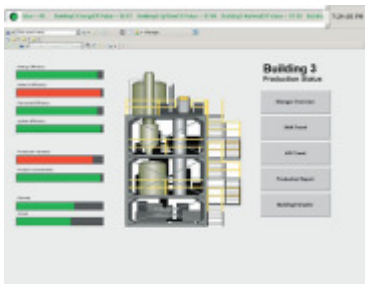


Figure 23

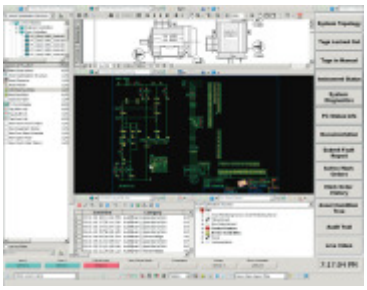


Figure 24

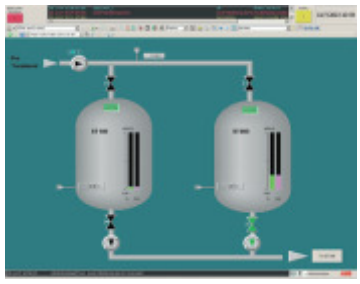


Figure 25

Another feature is the capability of Process Portal of integrating data from other SCADA or business applications into the process graphics and displays of system 800xA. It can also integrate useful data such as production and asset optimization data, security, etc… Other applications can also be launched from the Process Portal and commonly used file types can be opened (See Figure 26). Thus, from Process Portal the user has access to:

- Office.

- PDFs.
- Autocad engineering graphics.
- Real time video.

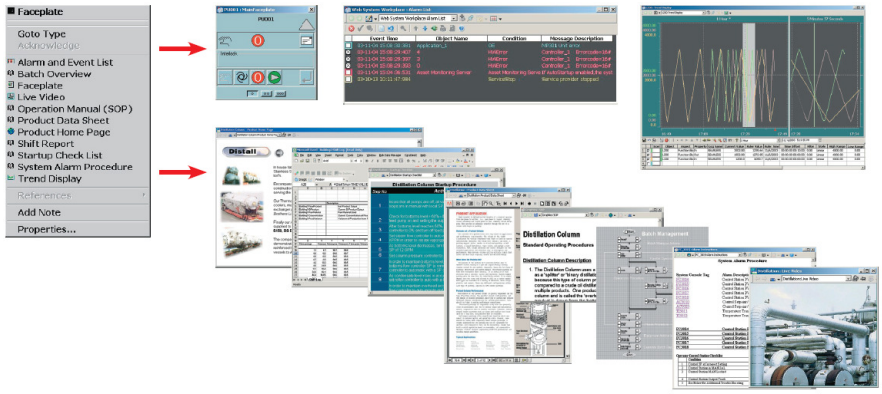


Figure 26

Another important feature is the alarm management. It has the usual options such as alarm priority schemes or automatic hiding and ignoring of alarms at some special moments, like plant starts and shutdowns. But it is also focused on showing all the available information to the operator so that the alarm or emergency situation is handled as quickly as possible. Thus, when the operator selects an alarm, the following information is presented:

- Process graphics and trends.
- Controller faceplate.
- Detailed procedures to handle the situation (HTML, Word or PDF format) (see Figure 27).
- Pop-up text windows and .wav or mp3 files can be played.
- SMS can be sent to cellular phones or paging systems and e-mails can be sent to notify the alarm.

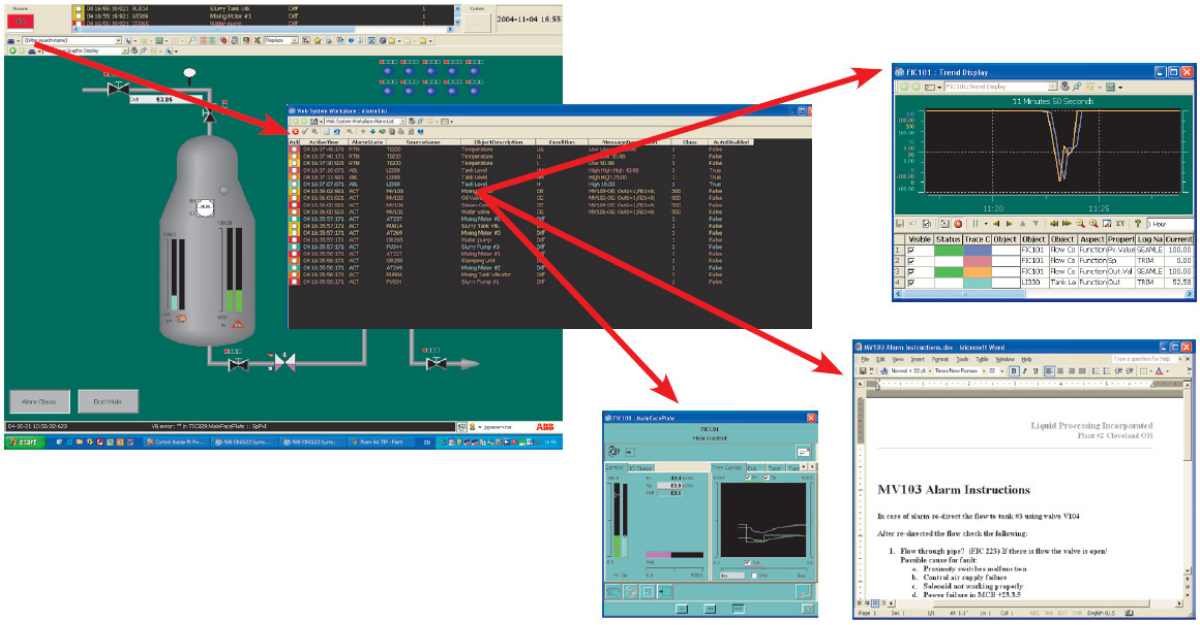


Figure 27

Finally, ABB (like Honeywell and Invensys) also has proprietary visualization systems tailored to system 800xA requirements (see Figure 29). The basic workstation of the Extended Operator Workplace is a curved display of 3x0.8 meters that can support up to three 800xA clients (see Figure 28).

Figure 29

Figure 28

1.2.4 Schneider

The most distinctive features of Vijeo are the fully functional visualization and the fact that operation can be performed from a web client (see Figure 30). Access to the HMI is controlled by the operator login which, in turn, has 3 different user profiles (operator,

management and engineering). Each object (process graphic, trend, etc.) has also been assigned a privilege level.

Figure 30

Vijeo has an extensive graphic library and supports display resolutions of up to 4096x4096 pixels in one or several displays. The configuration is based on objects (Genies and Super Genies: objects grouped in a page or pop-up window).

The module for alarms and process trend visualization is called Process Analyst (Figure 31). Having alarm and trends integrated in the same module makes the analysis of alarm causes easier and allows for a comparison of different batches, making the sequence of events that caused the alarm easier to understand.

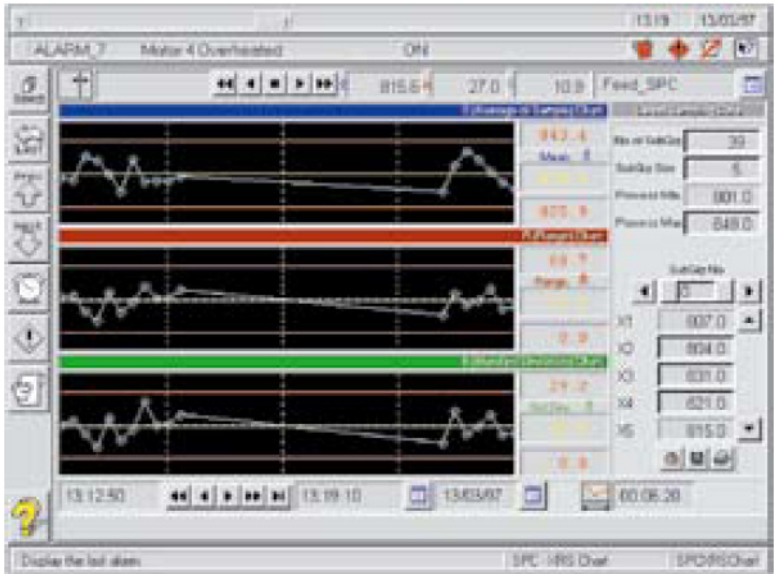


Figure 31

The alarm timing has an accuracy of 1 ms. and it is possible to filter alarms depending on their attributes. Furthermore, it guarantees that recent alarms are always visible to the operator.

Process Analyst can also be used to generate SPC (Statistical Process Control) graphics:

- Mean, range, standard deviation.
- Capacity plots.
- Pareto graphics.

Finally it is possible to show reports in Vijeo, but its capabilities are quite limited (there is an additional software package for this: Vijeo Historian).

1.2.5 Siemens WinCC

The software module used to build the HMI displays in WinCC is the WinCC Graphics Designer. This software allows HMI displays of up to 32 layers and 4096x4096 pixels. Library components and user defined objects can be added to these displays (see Figure 32 and Figure 33).

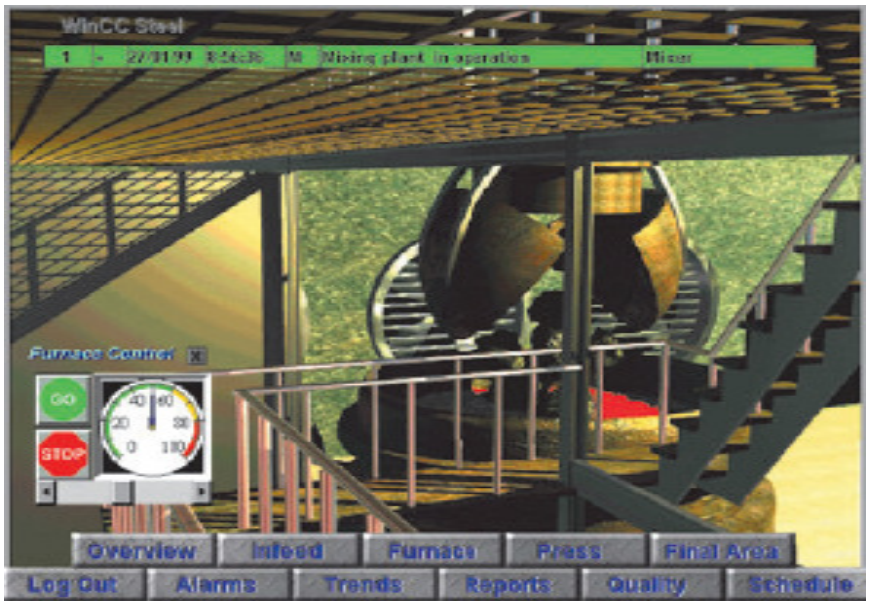


Figure 32

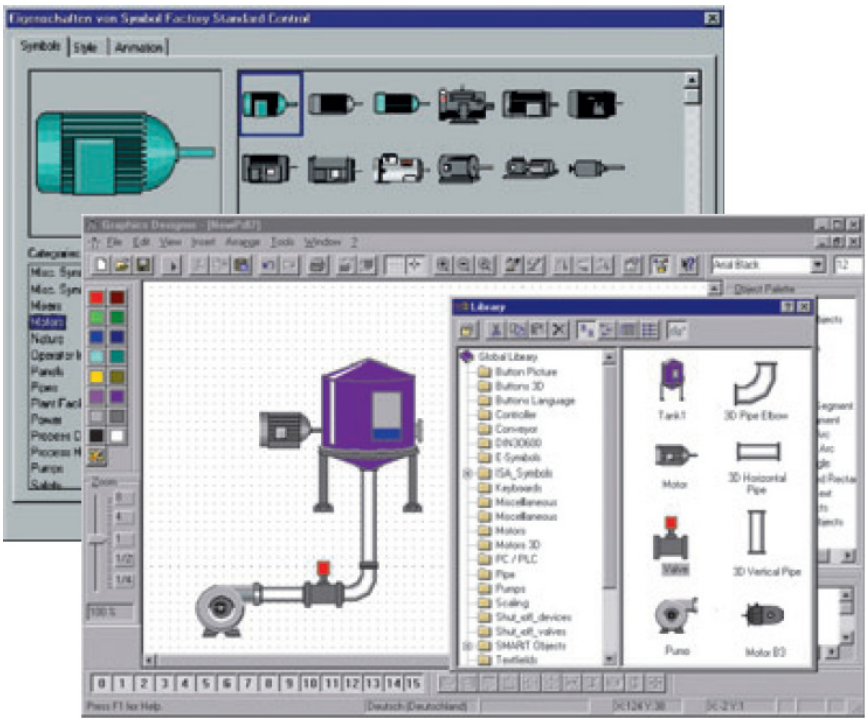


Figure 33

The display in WinCC is divided into a general zone, a work zone and a key zone. It also has hierarchical navigation and specific displays for each user. The alarm indications can be made by invoking an image of the component or process in which the event has happened and external alarm devices can also be triggered.

The module for analyzing trends is the WinCC Trend Control. It allows visualization of trends and real time data and can perform statistical operations over the historian data. The configuration of the trend graphics can be carried out on-line.

1.2.6 OASyS

XOS is the HMI of OASyS, and it has a very similar appearance to the Windows desktop:

- Tool bar in the upper zone.
- Status bar and alarm list in the lower zone.
- Main graphics in the center of the screen.

Geographical displays show the different components of the plant, with trend graphics, video (if available) and database data in real time. Alarms can be acknowledged individually or by groups and sound files can be associated to each alarm. Navigation is hierarchical, with layers that hide unnecessary details which, in turn, can be revealed by zooming into the object. The displays are designed using Autocad and a proprietary

software of Telvent that convert the Autocad drawings into HMI graphics. The use of Autocad, in spite of being more complex than other graphical editors, allows existing engineering drawings to be reused. OASyS has libraries with specific components and the configuration of the display is made with an editor that allows placing active content over the Autocad screen and linking portions of the drawing to the real time database.

1.3 Communication requirements

One aspect that must be discussed before analyzing industrial DCS networks is the network technology to be used. Network communications in control systems have been split traditionally into a plant network (usually based on Ethernet), a control network and a device network which was usually based on a field bus protocol. The actual trend is to extend the Ethernet technology to all three networks (see Figure 34). Thus, the hardware used in the networks of future control systems will be homogeneous throughout the architecture of the network. The use of "office" technologies over all networks results in a faster network, although recovery from a failure can be slower.

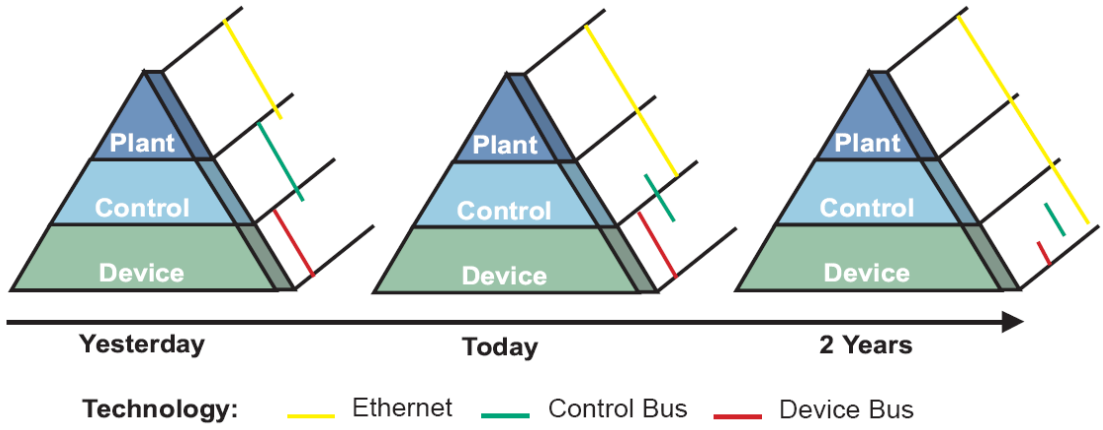


Figure 34

The bandwidth requirements must also be taken into account. Real time units usually require around 10 Kbps. However, communications between SCADAS need much more, up to 2 Mbps. Additionally, guaranteed quality of service (QoS) is necessary when other applications such as voice over IP and video streaming must be supported in the virtual network (VLAN) connecting all the SCADAs.

Another key point is network redundancy. Although redundancy is expensive, redundant networks are necessary and switching equipment with router capabilities are preferred to non routing capable switches. The topology of the redundant network will be chosen in function of the number of computers and devices connected to it. The most usual topologies are bus, ring, star and inverted trees.

1.3.1 Invensys

Invensys SCADAs can be built around any network topology or technology, but it is recommended to use Invensys's Mesh redundant network (see Figure 35). This is a redundant network built with conventional Gigabit Ethernet equipment. There is an Invensys software to manage redundant connections at every computer or device connected to the Mesh. This software is based on the RSTP (Rapid Spanning Tree Protocol) protocol.

Figure 35

The topology of the Mesh control network (and the physical layer) can be chosen in function of some aspects such as cost, size of the network or existing hardware. Thus the network topology can be a linear bus, a ring, a star or an inverted ring. The physical layer can be chosen to be shielded or unshielded twisted pairs or optic fiber cable.

The simplest case is the linear bus (see Figure 36). This network is built around two interconnected switches using Gigaethernet ports. All equipment in the network is connected to each switch using an Ethernet link. If one of the links for one of the switches fails, the network will continue working using the remaining link or switch.

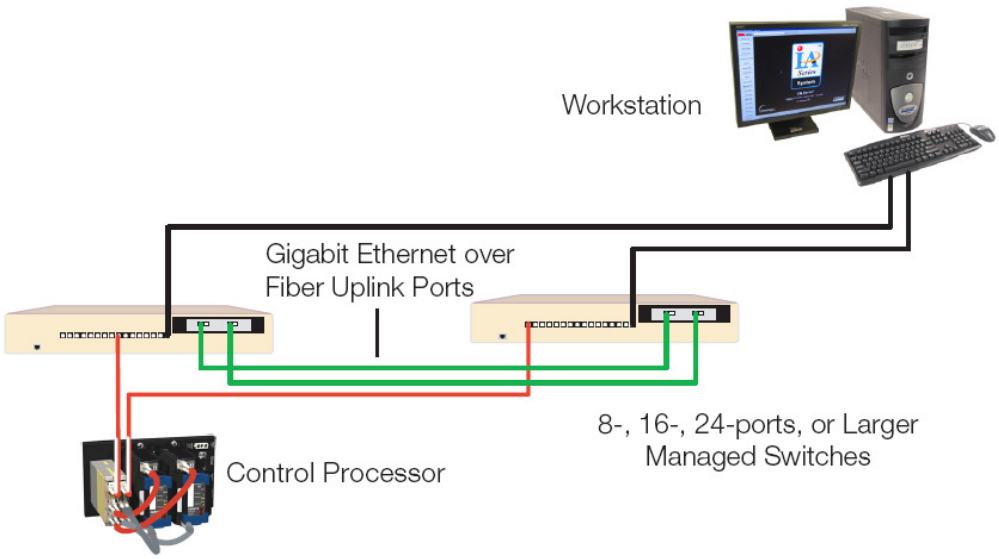


Figure 36

The linear bus topology is limited by the number of available ports at each switch and it is the best choice when the amount of equipment is not a problem.

The next step in complexity is the ring topology. In this topology, the switches are connected in a ring using Gigaethernet ports (see Figure 37) and all equipment is connected to two adjacent switches using redundancy management software. Thus, if one of the links fails, the network continues working without problems. A switch fail can also be managed, changing the topology to a linear bus. The RSTP protocol limits the number of switches in the equipment to seven. This fact together with the number of ports of each switch, limit the amount of equipment in this topology.

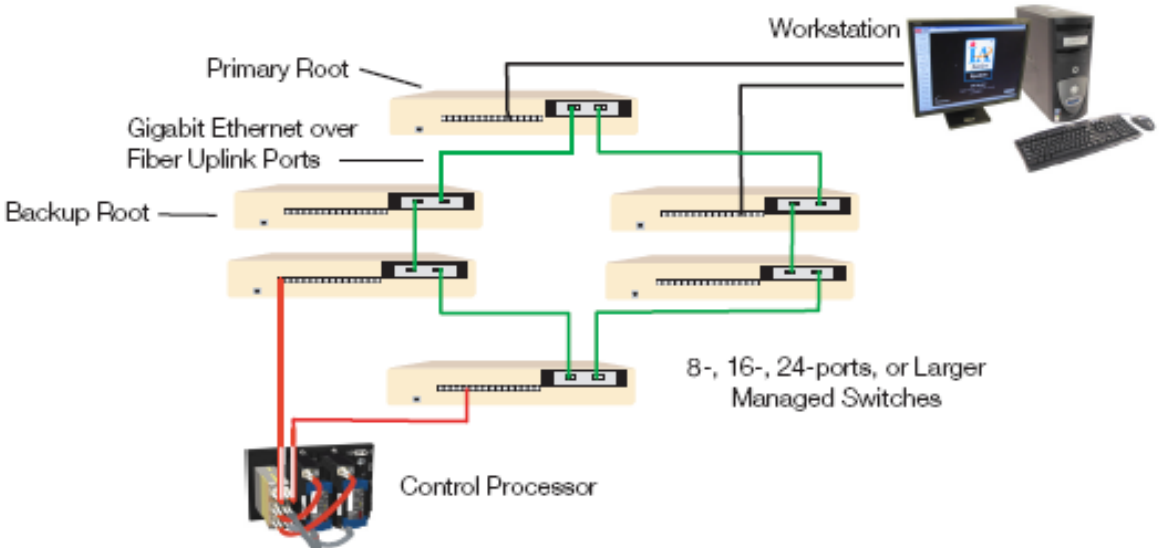


Figure 37

A redundant star topology can be used when the amount of equipment is high for ring topology. This topology consists of two routers or primary switches with a great backplane capacity and a number of secondary or edge switches that are connected to them (see Figure 38). The primary switches are connected to one another by two links. The equipment will be connected to two of the edge switches. A network with this topology keeps working without problems even when a link or a switch, primary or edge, fails. The maximum number of edge switches for each primary switch is 38, thus this topology is adequate for medium or large networks.

When the size of the network is very large, the inverted tree topology is the best option. In this case, there are up to four layers of switches (see Figure 39), so that each switch is connected to two of the next layer. The first layer is composed of two primary switches connected by a Gigaethernet link. The Gigaethernet links of the remaining switches are connected to the switches that have the same position in the adjacent layers. The equipment is connected to two of the switches of the last layer. This is the largest possible network supported by the Mesh Control Network of Invensys. The maximum size is:

- 250 Switches.
- 1920 work stations.
- Maximum recovery time of 1 second.
- 100 Mbps copper/fiber between the equipment and switch and switch to switch links of 1 Gbps. copper/fiber.

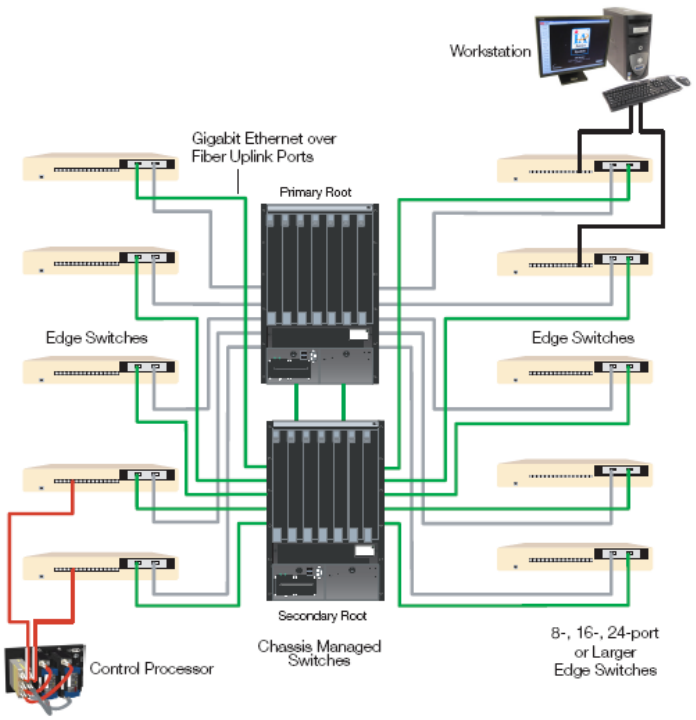


Figure 38

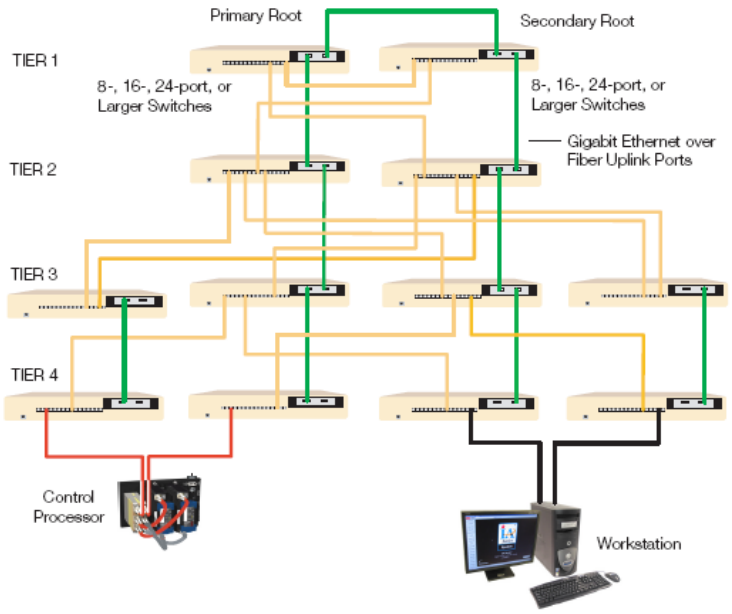


Figure 39

1.3.2 Honeywell

The proposal from Honeywell for a redundant network is a Fault Tolerant Ethernet (FTE). The main feature is that between each pair of nodes there are four possible routes, thus it is tolerant to multiple failures. The time required to detect and recover a failure is less than one second. Moreover, nodes without redundancy support can be connected to the FTE. Furthermore, the FTE is purely distributed without a master node and without duplication of the data sent through the FTE. Transmission speeds are 100 Mbps. over copper and 1 Gbps. over fiber.

The topology of the network consists of four redundant buses each one connected to the other, so that each one constitutes a level in the hierarchy of the network:

- Level 1: Real time control (RTUs and other field devices).
- Level 2: Supervisory control, human machine interface.
- Level 3: Advanced control (non critical control applications).
- Level 4: Plant level applications.

1.3.3 ABB

The redundant network of ABB is based on the same concepts as other networks, but in this case, redundancy and duplicity of resources is extreme (see Figure 40). Thus, in this case:

- Not only network links are redundant, but also power sources and even the CPUs of each real time unit (see Figure 41).
- Both data network (Ethernet) and field buses are redundant.
- Input-output units are also redundant.

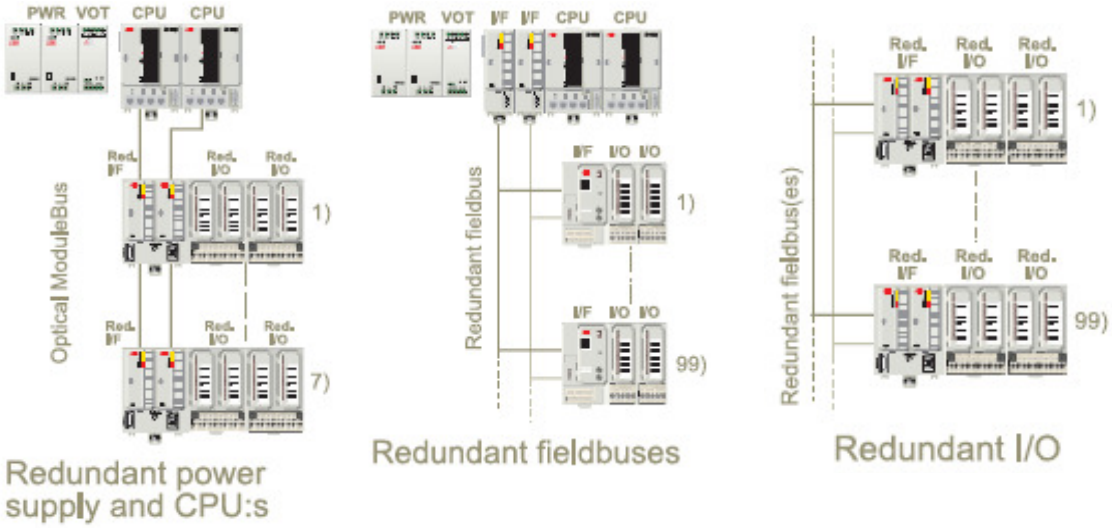


Figure 40

Figure 41

1.3.4 Schneider Vijeo

In this case, redundancy is considered with duplicate clients, servers, etc… but also there is a redundant network (see Figure 42). However, duplicity in clients and servers implies more licenses to buy. Redundant servers are in standby mirroring the primary servers until any of the primary servers fails. The redundant network is similar to the previous ones.

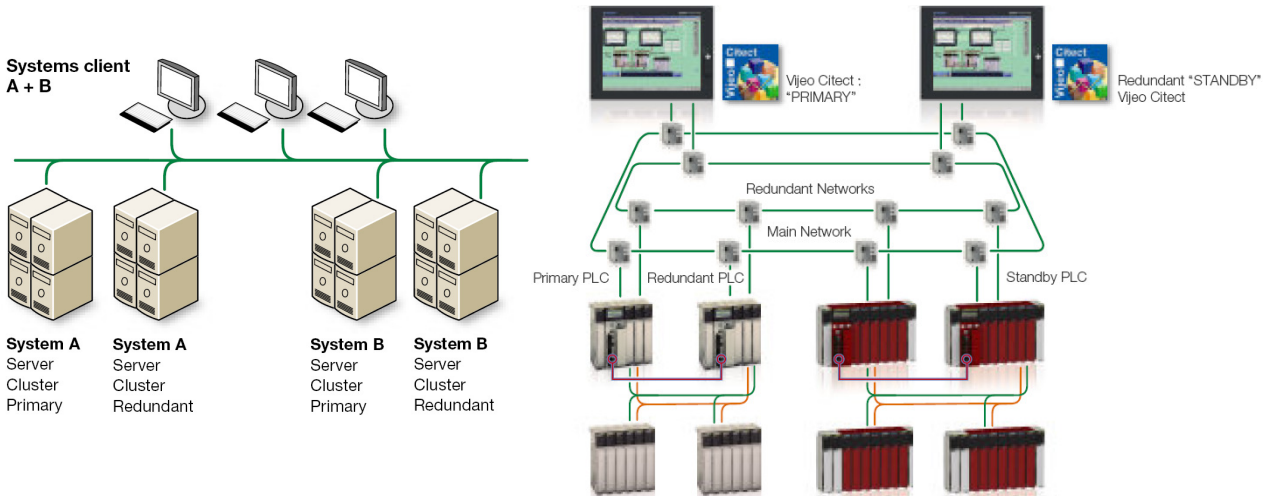


Figure 42

1.3.5 WinCC

WinCC redundancy is based (like other fault tolerant solutions) on duplicate servers that are connected through a redundant network. The software module WinCC/Redundancy is used to keep working in parallel two WinCC systems or two coupled servers. When the primary system fails, the secondary takes the primary role. When the primary is repaired both servers are synchronized (see Figure 43).

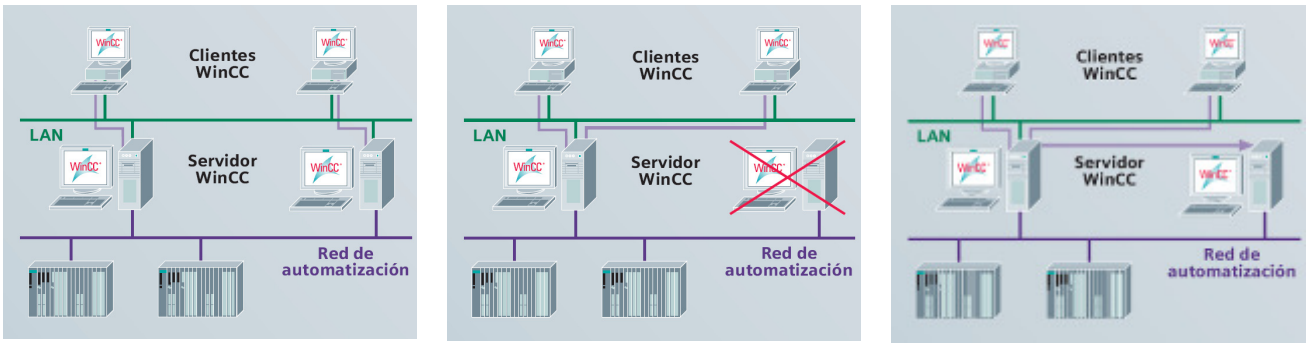


Figure 43

1.3.6 OASyS

OASyS has a redundant dual network that behaves as a virtual single network. It tolerates failure in any of its components. Switches are duplicated and two network interfaces are installed on all the equipment. It uses a floating IP addresses scheme so that the IP of the active server is assigned to the back-up one when the active fails. It has monitoring software that switches between active and back-up equipment when the active does not answer to monitoring messages. Large DCS can also be used with redundant WAN connections. Systems and data (historians, etc…) can be duplicated so that coherent and reliable data is always available.

1.4 Requirements summary

	Invensys InFusion + I/A	Honeywell Experion PKS	ABB 800xA + ECS	Schneider Vijeo	Siemens WinCC	Telvent OASyS DNA
Able to handle large systems composed of many large plants.	The I/A SCADA of each plant can handle 150000 objects (up to 50000 with triple redundancy).	Limited to 15 servers for each DCS and 40 stations for each one. A central control center can be configured using Uniformance PHD, Uniformance Process Studio and WorkCenter.	Up to 60000 tags per DCS. Apparently only one server for each DCS (single or redundant). Up to 40 local clients plus 15 remote clients for each DCS.	Apparently unlimited number of points, servers and clients.	Limited to 12 servers (each one with up to 64000 objects) and 32 clients.	Limits not available.
Integration of the information of the remote plants in a central control center.	Yes, using Infusion Access [4] (can access to virtually any commercial DCS).	Yes, its architecture is focused to a set of remote DCS and a central control center.	Yes, it can connect to other Systems through OPC, ODBC or proprietary interfaces. Information can be exchanged among the different DCS of each remote plant.	Although data can be exchanged through OPC and ODBC, the possibility of a central control center is apparently not considered.	It can connect to other SCADAs through OPC (Connectivity Pack). It lacks MES features.	It is possible to share data between different OASyS DCS and also with third party DCS through OPC. Data can also be remotely accessed from a web client.
SAP or ERP connectivity.	Yes, using OPC or ODBC.	It can be integrated with SAP and Office.	Yes, using ECS. Using only 800xA integration is limited to SAP PM (Plant Maintenance). It can be integrated with Office.	No. With Vijeo Historian it is possible to integrate with ORACLE.	Yes, using OPC Connectivity Pack. It can be integrated with Office and MS SQL using Industrial Data Bridge.	Yes, also with other software like MS Access, Lotus, Oracle, etc…
Open and flexible	Yes, it supports ODBC, OPC, HART, PROFIBUS, MODBUS, FDT and FieldBus.	Supports OPC, Profibus, Fieldbus, DeviceNet, LON,ControlNet, Interbus.	Supports ABB's propietary protocol, OPC, Profibus, Fieldbus and HART.	Apparently it can be connected only to Schneider equipments or use OPC.	Focused to SIMATIC S505/S5/S7. Also OPC and Profibus.	MODBUS, OPC.
Can handle Video-Wall or large multi-displays.	Yes with Enterprise Collaboration Wall and InFusion View. Proprietary I/A workstations.	Up to 4 displays (work spaces) at each workstation.	Workstations with up to 6 displays combined with 3 meters curved displays.	Conventional PCs with multi-display support and 4096x4096 pixels resolution.	Conventional PCs with resolution of up to 4096x4096 pixels (apparently without multi-display support).	No.
Able to operate any of the remote stations from the central control center with an unified HMI.	Yes, using an I/A client or InTouch (part of the wonderware suite). Remote actuation is not recommended.	Yes, Experion has DCS+ECS functionalities. Also from WorkCenter.	Yes using remote clients of DCS 800xA.	Only through OPC connectivity.	Limited by the maximum number of servers and clients (12/32 or 12/4).	Yes.

	Invensys InFusion + I/A	Honeywell Experion PKS	ABB 800xA + ECS	Schneider Vijeo	Siemens WinCC	Telvent OASyS DNA
Network topologies.	Switched Ethernet over copper and fiber. Bus, ring, star and inverted tree topologies.	Switched Ethernet over copper or fiber. Bus topology.	Ethernet over copper or fiber. Redundant bus topology.	Switched Ethernet over copper or fiber. Bus or ring topology.	Ethernet over copper or fiber. Bus topology.	Switched Ethernet.
Redundancy	Redundant network called Mesh Control Network. All the possible topologies are redundant..	Fault Tolerant Ethernet (FTE) with dual connections.	Different levels of redundancy: redundant buses, links, CPUs, power sources, etc…	Fault Tolerant Ethernet (FTE) with dual connections. Dual servers and dual cluster servers.	Dual servers, redundant links. Software WinCC Redundancy.	Redundant servers, links and networks. Transparent to the user.
OPC interfaces.	DA 1.0 and 2.04, HDA 1.0	AE, DA, HDA. There is an OPC module to bridge two DCS servers.	DA, AE and HDA.	DA 2.0.	DA, HDA, AE, XML (the latter three Orly with connectivity pack).	DA 2.0.

2 Industrial Wireless Sensor Networks

Traditionally, industrial automation systems are implemented through wired communications. The installation and maintenance costs of cabling many (possibly distant) sensors impose restrictions on the maximum number of sensors that can be installed in an industrial control application. Wireless communication represents therefore a major industrial challenge in the coming years. It offers numerous usages and helps industry save operating costs as well as improving operational efficiency. General-public wireless technologies (i.e., WIFI and Bluetooth) may find their usage limited in industrial installations because of harsh environments, electromagnetic compatibility and interference issues, safety and information technology (IT) security constraints, and battery autonomy. However, with the recent advances in wireless sensor networks (WSNs), the implementation of low-cost embedded industrial automation systems has become feasible. In these systems, wireless sensor nodes are installed in industrial equipment and monitor parameters such as vibration, temperature, pressure, and power quality. These data are then wirelessly transmitted to a sink node that analyzes the data from each sensor. Wireless sensor networks have some interesting characteristics such as self-organizing and auto-configurable topology, and *ad hoc* routing concept. These properties promise substantial benefits in terms of operating and maintenance costs of the communication infrastructure in industrial installations. Also, the fact that the number of installed sensors can grow may enable significant savings and reduce air-pollutant emissions by optimizing the management of industrial systems.

Challenges and design requirements in Industrial Wireless Sensor Networks as outlined in[23,24] are:

a) The fundamental resources (energy, memory capacity and computing capabilities) are constrained due to the limited physical sizes of sensors and the dependence on batteries. Thus, a resource-efficient design is necessary maximizing network lifetime while providing the QoS required by the application.

b) Dynamic topologies and harsh environmental conditions. The topology and connectivity of the network may vary due to link and sensor-node failures. Furthermore, sensors may also be subject to RF interference, highly caustic or corrosive environments, dirt, etc… that may cause malfunction of the sensor nodes. To fight against this, network operation must be adaptive to cope with dynamic/varying wireless-channel conditions in industrial environments and to balance the tradeoffs among resources, accuracy, latency, and time synchronization.

c) Quality-of-service (QoS) requirements. The QoS provided by IWSNs refers to the accuracy between the data reported to the sink node (the control center) and what is actually occurring in the industrial environment. In addition, it is important to receive the data at the sink in a timely manner. To meet QoS requirements some principles must be taken into account. Firstly, in IWSNs, a one-size-fits-all solution does not exist; instead, custom designs should be developed based on the application-specific QoS requirements and constraints.

Secondly, time synchronization is fundamental*:* in IWSNs, large numbers of sensor nodes need to collaborate to perform the sensing task, and the collected data are usually delay-sensitive.

d) Data redundancy. Because of the high density in the network topology, sensor observations are highly correlated in the space domain, thus redundancy in the information that it is sent through the network can be very high. This can be reduced using data fusion and localized processing. Instead of sending the raw data to the sink node directly, sensor nodes can locally filter the sensed data and transmit only the processed data, reducing the communication overhead.

e) Packet errors and variable-link capacity. In IWSNs, the attainable capacity and delay of each wireless link depends on the interference level perceived at the receiver, and high bit error rates are observed in communication. On the other hand, fault tolerance and reliability should be guaranteed. However, the sensed data are exchanged over the time-varying and error prone wireless medium. Thus, data verification and correction at each communication layer and self-recovery procedures are extremely critical to provide accurate results to the end-user.

f) Security. The network design must make communication safe from external denial-of-service (DoS) attacks and intrusion, but there are other types of security attacks. Passive attacks are carried out by eavesdropping on transmissions including traffic analysis or disclosure of message contents. Active attacks consist of modification, fabrication, and interruption, which in IWSN cases may include node capturing, routing attacks, or flooding. To prevent these attacks, the network design must have security mechanisms both low-level (key establishment and trust control, secrecy and authentication, privacy, robustness to communication DoS, secure routing, resilience to node capture) and high-level (secure group management, intrusion detection, secure data aggregation). All these security mechanisms, however, must have the minimum computing overhead.

g) Large-scale deployment and ad hoc architecture. Usually, an IWSN will contain a large number of sensor nodes randomly spread over the deployment field. The large number of sensor nodes (from hundreds to thousands) requires a low-cost and small design of such sensor nodes. The cost per sensor is the total cost of ownership (packaging requirements, modifications, maintainability, implementation, etc.), and training and servicing costs as well. On the other hand, network infrastructures are usually nonexistent, thus node connectivity must be maintained autonomously. Also, the dynamic topologies caused by node failure/mobility/temporary power-down and large-scale node deployments necessitate self-organizing architectures and protocols. Thus, self-configuration and self-organization are desirable features so that those changes do not affect the general objective of the application.

h) Integration with Internet and other networks. It is important to be able to retrieve useful network information from anywhere and at any time. For this reason, the IWSNs should be remotely accessible from the Internet. The current sensor-network platforms use gateways for integration between

IWSNs and the Internet. Also, the IWSNs must support heterogeneous industrial applications with different requirements. In addition, interoperability with existing legacy solutions, such as fieldbus and Ethernet-based systems, is required. Thus, it is necessary to develop flexible and scalable architectures that can accommodate the requirements of all these applications in the same infrastructure.

2.1 Existing industrial wireless communication standards

2.1.1 ZigBee

ZigBee is a networking standard based on IEEE 802.15.4 radio technology targeted at industrial control and monitoring (it is designed to interconnect autonomous sensors and actuators to control units) building and home automation, embedded sensing, and energy system automation. ZigBee is promoted by a large consortium of industry players, including Motorola, Texas Instruments, Philips, Samsung, Siemens, Freescale and others. It proposes a lightweight protocol stack (taking only 32 or 64 Kb depending on the role of the node) for applications which require low data rates (up to 250 kb/s) and low latency. Power-saving modes are very efficient yielding battery lifetime from a few months to many years.

ZigBee is based on IEEE 802.15.4-2003 physical (868 MHz/915 MHz or 2.4 GHz) and MAC layers over which it specifies its network layer and the application layer (Figure 44). The network layer specifies routing and security mechanisms as well as those used to join and leave a network. Discovery and maintenance of routes between devices is achieved by discovering adjacent neighbors and storing relevant neighbor information. The network topologies can be star, tree or mesh. In a star topology, the network is controlled by one single device called the ZigBee coordinator. In mesh and tree topologies, there are ZigBee routers (that can be used to expand the network), but the ZigBee coordinator is still responsible for starting a new network and assigning addresses to joining devices. In tree networks, routers transfer data and control messages through the network using a hierarchical routing strategy. This routing strategy is a mixed mechanism composed of a simplified version of ad hoc on-Demand Distance Vector (AODV) and tree routing intended to extend the coverage of the network beyond the coverage of each network node.

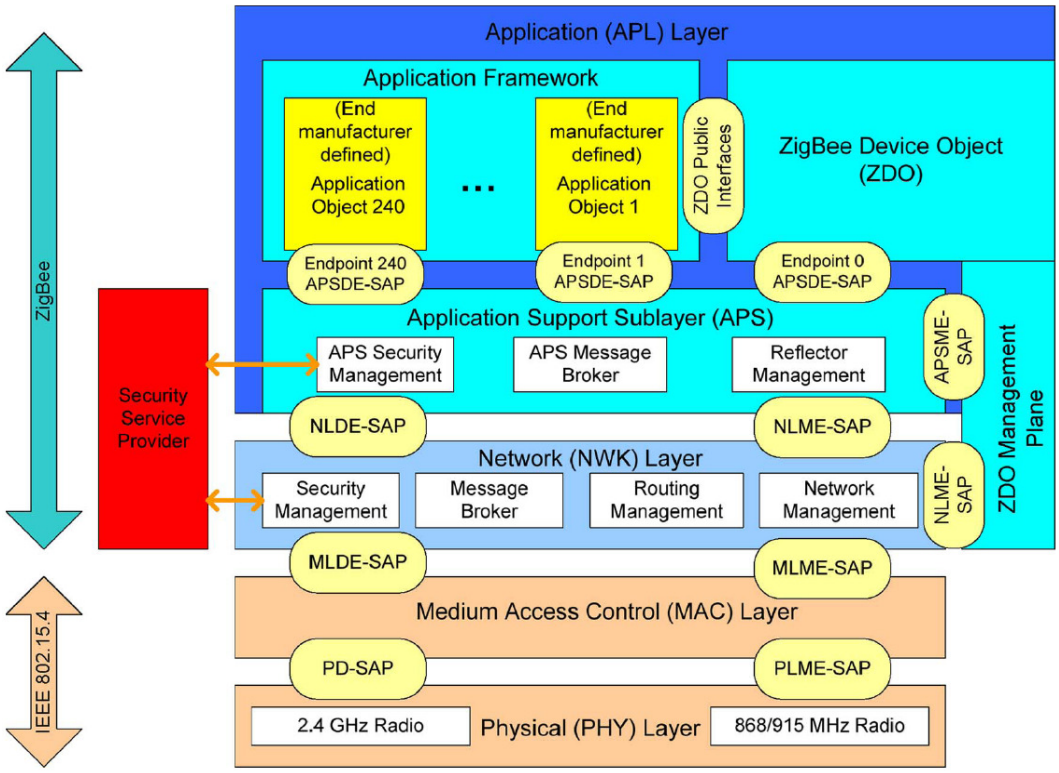


Figure 44

The ZigBee application layer is composed of application support sub-layers, the ZigBee device object, and the manufacturer-defined application objects. The application layer is used to:

- Maintain the tables for binding (i.e. for matching two devices together based on their services and their needs).
- Forwarding application messages between bound devices.
- Defining the role of the device within the network (ZigBee Coordinator, Router, or End device).
- Discovering devices on the network, determining which application services they provide, initiating and/or responding to binding requests, and establishing a secure relationship between network devices.

The medium access method of ZigBee is based on the uncoordinated mode of the IEEE 802.15.4 standard. This mode requires the ZigBee coordinator to listen permanently to the channel and, thus, wastes the coordinator battery. Energy is saved mostly in the end devices which have a very low power consumption in “doze” mode (lower than 10 μA.), and letting them switch to normal operating mode in less than 300 μs.

Although ZigBee is used for IWSNs, it has some drawbacks to be considered:

1) Battery autonomy is not enough for wireless sensor networks in application such as environmental monitoring in large industrial facility. Due to the uncoordinated mode of medium access, only ZigBee End Devices can be put in doze mode. ZigBee Routers and Coordinators need to be always awakened (active mode).

2) Another limitation of ZigBee is that it does not directly support device mobility. AODV only discovers the route on demand and the only used QoS is the instantaneous radio link, thus, route repair is done on error. The complete route-discovery process can take a significant time (up to 10 s), too much for industrial applications.

3) ZigBee does not offer support for sink mobility in which data-collector points travel through the nodes of a wireless sensor network.

2.1.2 ISA 100

The ISA100 working group is focused on a reliable wireless communication system for monitoring and control applications, taking the special demands of the process industry into account. Specifically, the focus here is to address performance needs for periodic monitoring and process control where latencies on the order of 100 ms can be tolerated with optional behavior for shorter latency. This group is currently working on a standard (the first release has been approved very recently) which will lead to an interconnectivity of wireless solutions for the industry automation. Coexistence with WiFi is also taken into account, and that is really appreciated in industrial environment. This standard, named ISA100.11a, is developed by different organizations and alliances such as the Wireless Industrial Network Alliance (WINA), NCCR-MICS, NSF-Program on Sensors and SeNetworks and HCF. ISA100.11a Working Group3.

The ISA100.11a is focused to fulfill the following requirements:

1) Able to be used in both process-industry applications and factory automation.
2) Able to be used in in-plant and near-plant networks.
3) Technology to address different traffic class.
4) A single application layer providing both native and tunneling protocol capability for broad usability.
5) The addressing of 2.4 GHz IEEE 802.15.4-2006 physical layer devices.
6) A comprehensive coexistence strategy with channel hopping to support coexistence (with IEEE 802.11) and increase reliability.
7) Simple, flexible, and scalable security addressing major industrial threats leveraging IEEE 802.15.4-2006 security.
8) Field-device meshing and star capability.

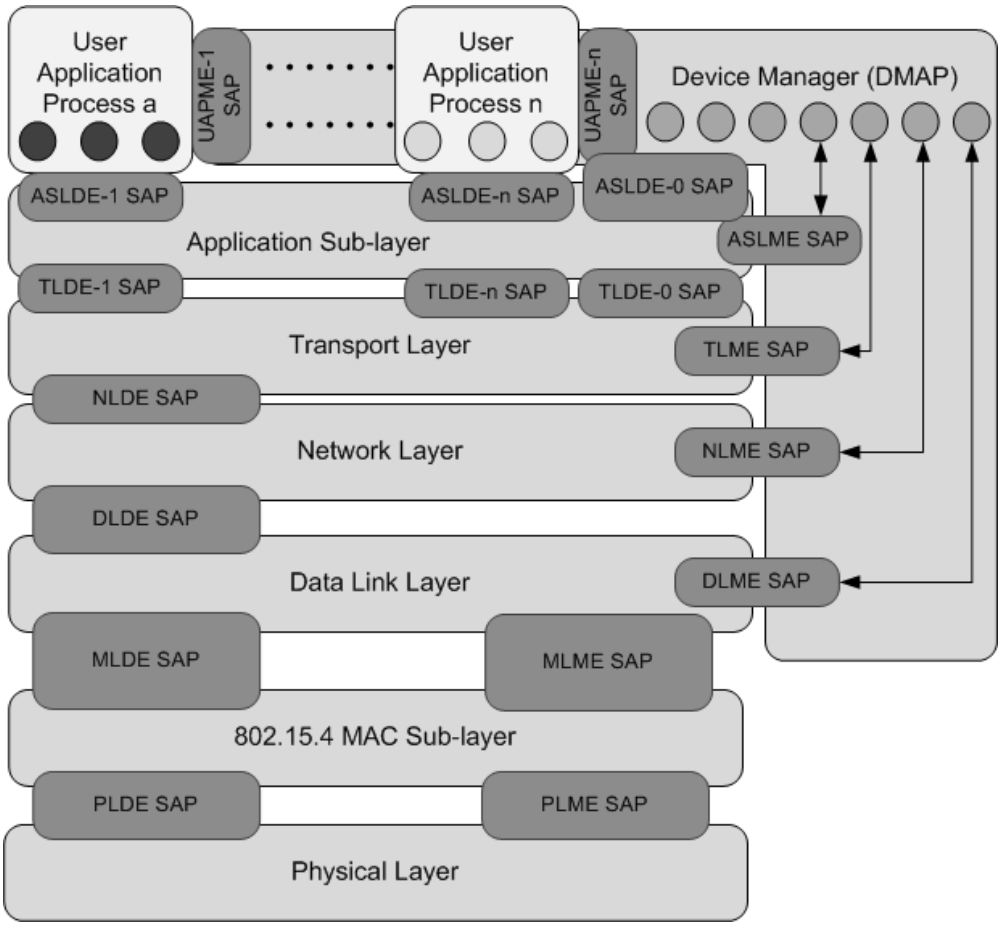


Figure 45

ISA100.11a stack architecture (see Figure 45) has more layers than the ZigBee one. This may impose technical difficulties to implement the full stack architecture on low cost hardware. The device-management application process (DMAP) can directly access (using service access point) to the Data-Link Layer, the Network Layer, the Transport Layer, and the Application Sub-layer in order to manage the device and its communication services. The DMAP provides a basis for building system-management-configuration application and communication-monitoring application.

The network configuration has a series of wireless field devices (see Figure 46), some of them can route messages, and others may not have routing capabilities or may not be configured to use routing capabilities. The network is attached to a user application at a gateway. The gateway provides the transition from ISA100.11a into the users' application.

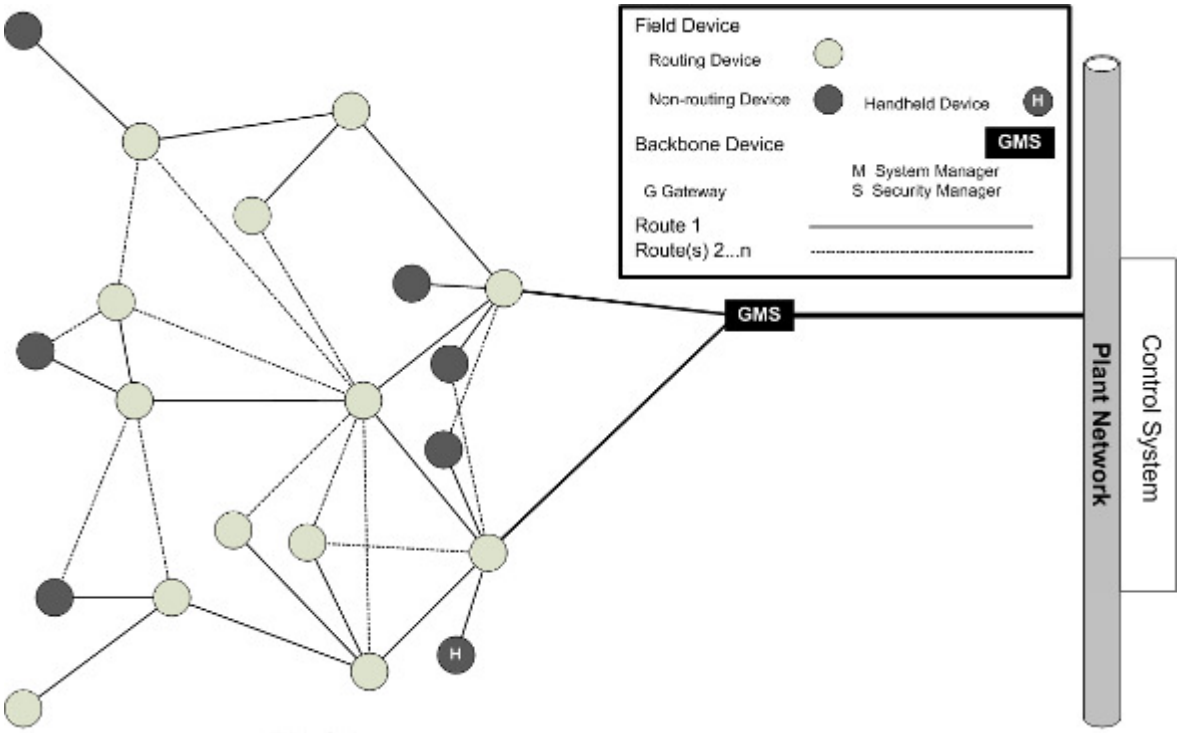


Figure 46

Two main classes of devices are defined in ISA100.11a: Field Devices and Backbone Devices. Field Devices can have, but not necessarily, routing capability. For example, a handheld device is considered as a non-routing field device. Roaming of handheld device is not supported by ISA100.11a. Backbone devices (e.g. the gateway) are full-function devices which are continuously powered, whereas field devices have limited battery power (without routing capability) or moderate power (with routing capability).

ISA100.11a addresses failed communications using *frequency and slotted-hopping* architecture by adding a MAC Extension Shim to the IEEE 802.15.4 MAC. Security is also other important focus of ISA100.11, which provides authentication, encryption, and authorization services**.** The communications security functionality for ISA100.11a is primarily transmission security with authorization based on device identity and configured plant communications relationships. Transmission security is provided for the MAC sub-layer and for the transport layer:

- MAC security defends against attackers who are outside the system and do not share system secrets.
- Transport security defends against attackers who are already inside the system and have co-opted (i.e., Trojans) some devices.

The types of keys supported include both symmetrical keys and non-symmetrical (i.e. public) keys.

Network time and time-synchronization information for devices on the network are provided by the system manager, a particular backbone device, which acts as clock source. Routing in ISA100.11a is based on graphs using a directed list of links that connect devices. The links associated with each graph are configured by the system-management function on a centralized or decentralized basis. A single network instance may have multiple graphs, some of which may overlap. Each device may have multiple graphs going through it, even to the same neighbors. Each device data-link layer service has one route associated with it. Currently, there is no optimized routing strategy for maximizing the lifetime of field network.

2.1.3 Wireless HART

*Wireless*HART is a wireless mesh network communication protocol for process automation applications. It adds wireless capabilities to the HART Protocol while maintaining compatibility with existing HART devices, commands, and tools.

Wireless HART was added to the overall HART protocol suite as part of the HART 7 Specification, which was approved by the HART Communication Foundation in June 2007. The HART protocol is a digital-communication technology that is designed for process measurement and control devices.

Each ***WirelessHART network*** includes three main elements (see Figure 47)**:**

1. **Wireless field devices** connected to process or plant equipment. This device could be a device with WirelessHART built in or an existing installed HART-enabled device with a WirelessHART adapter attached to it.

2. **Gateways** enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.

3. **A Network Manager** is responsible for configuring the network, scheduling, communication between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, the host application, or the process automation controller.

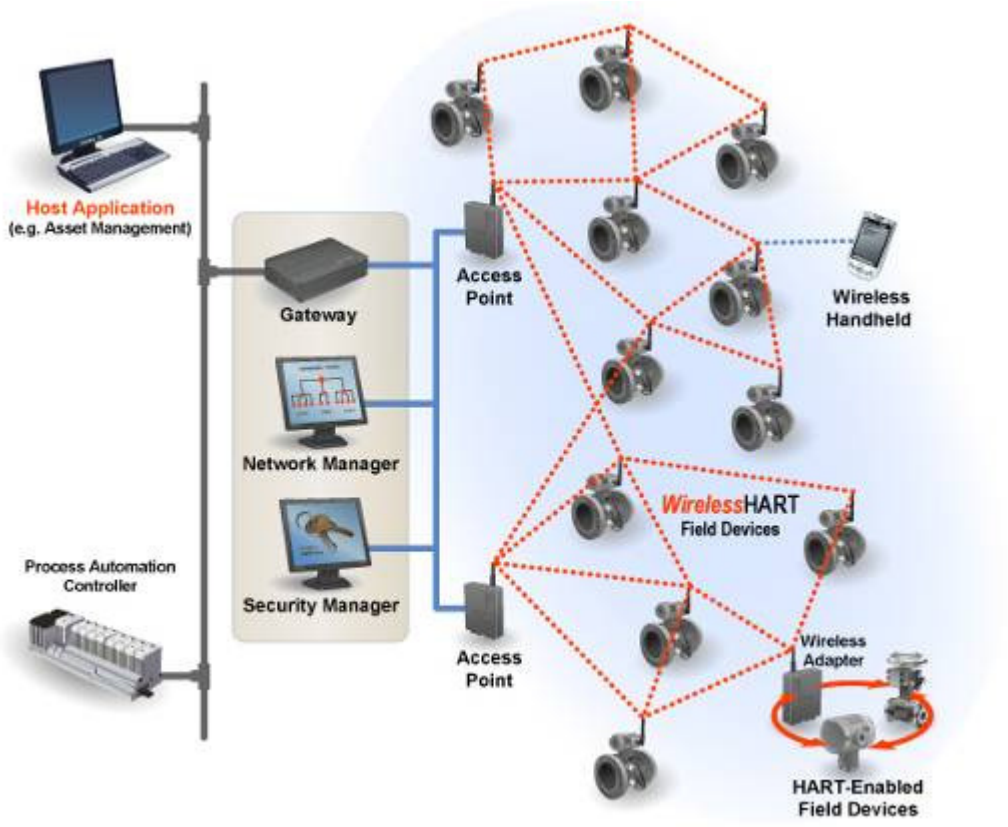


Figure 47

The network uses IEEE 802.15.4 compatible radios operating in the 2.4GHz Industrial, Scientific, and Medical radio band. The radios employ direct-sequence spread spectrum technology and channel hopping for communication security and reliability, as well as TDMA synchronized, latency-controlled communications between devices on the network. This technology has been proven in field trials and real plant installations across a broad range of process control industries.

Each device in the mesh network can serve as a router for messages from other devices. In other words, a device doesn't have to communicate directly to a gateway, but just forward its message to the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability.

The **Network Manager** determines the redundant routes based on latency, efficiency and reliability. To ensure that the redundant routes remain open and unobstructed, messages continuously alternate between the redundant paths. Consequently, like the Internet, if a message is unable to reach its destination by one path, it is automatically re-routed to follow a known-good, redundant path with no loss of data.

The mesh design also makes easy adding or moving devices. As long as a device is within range of others in the network, it can communicate.

For flexibility purposes and to meet different application requirements, the *Wireless*HART standard supports multiple messaging modes including one-way

publishing of process and control values, spontaneous notification by exception, ad-hoc request/response, and auto-segmented block transfers of large data sets. These capabilities allow communications to be tailored to application requirements thereby reducing power usage and overhead.

The components of the *Wireless*HART technology are:

- A **Gateway** provides the connection to the host network. WirelessHART and then the main host interfaces such as Modbus – Profibus – Ethernet. The Gateway also provides the network manager and security manager (these functions can also exist at the host level – however initially they will be in the gateway).
- **The Network manager** builds and maintains the MESH network. It identifies the best paths and manages distribution of slot time access (WirelessHART divides each second into 10msec slots) Slot access depends upon the required process value refresh rate and other access (alarm reporting – configuration changes)
- The **Security manager** manages and distributes security encryption keys. It also holds the list of authorized devices to join the network.
- The **Process** includes measuring devices – the HART-enabled instrumentation.
- A **Repeater** is a device which routes WirelessHART messages but may have no process connection of its own. Its main use would be to extend the range of a WirelessHART network or help "go around" an existing or new obstacle (New process vessel). All instruments in a WirelessHART network have routing capability which simplifies planning and implementation of a wireless network.
- The **Adapter** is a device which plugs into an existing HART-enabled instrument to pass the instrument data through a WirelessHART network to the host. The adapter could be located anywhere along the instrument 4-20mA cable; it could be battery powered or obtain its power from the 4-20Ma cable. Some adapters will be battery powered and use the same battery to power the instrument as well – in this case there will be no 4-20mA signal to the host – all process data will be reported via *Wireless*HART
- A **Handheld Terminal:** There are two versions: In the first one, the handheld will be a standard HART FSK configuration unit (just add new device DDs or DOF files), just like the one used for everyday tasks such as routine maintenance and calibration checks. In the case of wireless support, the handheld is used to join a new instrument to an existing *Wireless*HART network. In the second case the handheld has a *Wireless*HART connection to the gateway and then down to an instrument and could be used for reading PV or diagnostics.

Security in *Wireless*HART is kept by using a multi-key architecture based on industry-standard, AES-128 block ciphers with symmetric keys: Separate join key per device.

- Network key to authenticate Data-Link PDUs.
- Session keys encipher network payloads ensuring private, un-molested communication between end-point devices.

- Key management is delegated to the user and may be as simple or complex as required by plant policy.
- Only trusted devices are allowed to join the network.
- Trusted device identified by Join key and standard HART Identity data (i.e., Manufacturer ID, Device Type, Device ID, Tag, etc.).

*Wireless*HART is much more focused to industrial control applications than ZigBee, but has some weak points like the fact that it does not specify any energy-aware *ad hoc* routing strategy in its network layer.

2.2 Operating systems

When designing an operating system for IWSNs it is very important to balance the tradeoff between energy and QoS requirements. In this regard, TinyOS is one of the earliest operating systems dedicated to tiny sensor nodes. Originally developed by the University of California, Berkeley and Intel at the beginning of the decade, it has since become the most popular operating system for wireless sensor networks. Its open-source nature and large user-base make it the de facto standard for this class of devices.

It incorporates a component-based architecture, which minimize the code size and provides a flexible platform for implementing new communication protocols. It fits in 178 KB of memory and supports communication, multitasking, and code modularity. In the following the main aspects of TinyOS will be reviewed. Most data will be for versions 1.x, as they are the most extended in commercial sensor platforms as those from Crossbow. Some details about the new 2.x versions will also be given.

2.2.1 TinyOS 1.x

TinyOS [27,28,29,30] is one of the first execution environments specifically designed to meet the requirements of resource-constrained, event-driven and networked embedded systems. It is one of the most popular operating system for wireless sensor networks and it is used by commercial brands like Crossbow and Moteiv (now Sentilla), and also by research platforms like BTnode. Its open-source nature and its large user-base make it the de facto standard for this class of devices.

One of the main characteristics of TinyOS is the use of component modularization. The functionality of the traditional monolithic abstraction layers is broken-up in smaller, self-contained building blocks that interact with each other via clearly defined interfaces. This preserves the modularity of the applications and promotes reuse of code. The interactions between the building blocks are not only of up/down nature, they also resemble a graph. In this way, more complex relationships can be modeled. This component paradigm fits very well to the event-driven nature and the constrained resources of an IWSN. The applications are then composed by wiring together the necessary building blocks.

Another important aspect that defines the applications organization is the concurrency model. It must allow the asynchronous and event-driven type of exchange that occurs not only in communications but also in the applications as they are usually triggered by some sensed event. Also, the operating system must take into account the limited hardware resources. The TinyOS solution offers two levels of concurrency: tasks and events. Tasks have deferred computation and should be used whenever the timing requirements for the computation are not strict. Components can post a task, after which the execution immediately returns. However, the actual execution can be delayed until it is attended by the task scheduler (which runs with a FIFO task scheduling policy). Tasks run to completion and do not preempt each other in order to keep the overhead of context-switching at a minimum. This implies that they must be short to get low task execution latencies. Furthermore, events also run to completion, but can preempt the execution of tasks and/or other events. Events can represent hardware interrupts, or be used to signalize the completion of a split-phase operation.

As TinyOS is non-preemptive, blocking operations are not supported and long-latency operations have to be realized in a split-phase fashion, by separating the operation-request and the signaling of the completion. A client requests the execution of an operation using a command handler in the server. The server signals the completion of the operation by calling an event handler in the client. In this way, each component involved in the interaction is responsible for implementing part of the split-phase operation.

The simple concurrency model of TinyOS has the benefit of keeping the overhead significantly lower than in the traditional thread-based approaches. However, typical programming errors occurring in concurrent systems including deadlocks and data-races are not avoided. These errors can be fatal in an IWSN where there can be no human-operator in the control-loop mitigating actions. The preferred programming language of TinyOS, NesC [26], imposes several restrictions to reduce the chance of introducing complex bugs. For example, it does not support dynamic memory allocation or function pointers. Consequently, the call-graph of NesC programs is fully known at compile-time, allowing NesC to perform whole-program analysis for safety and performance optimization, avoiding almost all potential data-races.

TinyOS has been designed to allow some software components to be replaced with real hardware modules (that export the same interfaces) and vice versa. The core component categories involved in abstracting the supported hardware platforms in TinyOS 1.x are:

- **Micro Controller Unit core:** The NesC/C programming language hides most of the differences between the controller core architectures. The standard C library creates the necessary start-up code for initialization of global variables, the stack pointer and the interrupt vector table.
- **Pins:** Using macros it is possible to set and clear I/O pins as well as changing the direction and function.
- **Clocks and timers:** The top-level timer service in TinyOS 1.x, exported by the TimerM component, provides timed periodic and one-shot millisecond-resolution events, multiplexed from a single hardware timer compare register.
- **Analog-to-digital converters and sensors:** In the early versions of TinyOS 1.x there were only commands for triggering a single or repeated conversion

from one input channel. This has been rectified with the new abstractions introduced in later versions and thus it is possible to reconfigure the hardware for each sampling command.

- **Data buses:** TinyOS provides abstraction for several standard data buses like SPI/USART, UART, I^2C, 1-Wire, etc. The abstraction is usually organized in two paths, one for data and the other for control. The data interface allows sending and receiving bytes via the registers of the particular data-bus module. The control path allows enabling or disabling some components or parameters like the clock source, generation of interrupts, baud-rate, etc.,
- **External storage** The secondary memory is interfaced to the micro controller using one of the data buses. It is possible to access to a single memory cell or using more complex abstractions read or write entire blocks.
- **Radios:** The component organization of the radio chip abstractions mainly depends on the particular data interface that the radio supports. The basic data unit (bit, byte or packet) is usually directly exposed by the lowest level components. The control of the radio is performed using a combination of hardware pins and control registers that are accessed using the data bus abstractions.

Finally, the networking services of TinyOS 1.x will be briefly reviewed in the following paragraph. They are mainly represented by active messages, which consists of a small identifier that is attached to each message, specifying the action that needs to be taken on the receive side. They are similar to the port concept in a TCP/IP stack. The lower parts of the networking stack are generally encapsulated in an abstraction called GenericComm that provides single hop unicast and broadcast service. The basic multi-hop communication pattern supported in TinyOS is the reverse-tree routing. A single node is selected to act as a root node. Each node in the network selects a parent node that is used for forwarding the messages back to the root and maintains its depth in the tree in the form of a hop-count to the root. The tree-routing protocols can differ in the way that this structure is constructed and used. In the early versions of TinyOS, the approach to build the tree was active, issuing periodic floods from the root to maintain the topology. Newer versions rely on snooping the forwarded messages between the nodes and their parents. This is used to create candidate-parent tables from which a new parent can be selected when the connection with the current one is broken or does not satisfy a predetermined quality metric.

2.2.2 TinyOS 2.x

The second generation of the mote operating system keeps many of the basic ideas of its predecessor while pushing the design in key areas like greater portability and improved robustness and reliability [33]. In the following a brief revision of the major changes introduced in the newer versions is presented.

Portability has been enhanced by introducing a three-layer Hardware Abstraction Architecture. The lower layer is the Hardware Presentation Layer that provides access to basic resources such as registers, interrupts and pins. The middle layer is the Hardware Abstraction Layer which provides useful abstractions of the full capabilities of the underlying hardware. The top layer is the Hardware Independent Layer which, as its name suggests, is composed by hardware independent abstractions that can be

easily ported among different hardware platforms. Also, due to the fact that wireless sensors are usually built from standard chips, TinyOS 2.0 introduces the concept of "abstract" chips to allow reuse of subsystems corresponding to these chips across different platforms. Portability is also improved with the newer versions of the NesC language, which introduce the notion of network type at the language level: programs can declare "structs" and primitive types that follow a cross-platform (1-byte aligned, big-endian) layout and encoding. This allows services to specify cross-platform packet formats.

Reliability and robustness have also been improved in TinyOS 2.x by redefining some of the basic TinyOS abstractions and policies such as initialization, the task queue, resource arbitration and power management. In TinyOS 2.0, every task has its own reserved slot in the queue and can be posted only once. The new semantics lead to greatly simplified code (no need for task reposting on error) and more robust components.

The static nature of TinyOS 1.x has been further increased in the newer versions. Components allocate all of the state they might possibly need; and all invariants are explicitly reflected by the components and their interfaces, rather than being checked at runtime. The idea behind this is to make the system more deterministic, even when this leads to a loss of flexibility. Other things have been improved, such as the timer system, the active messages, the sensor and serial stack, and also new default dissemination and collection protocols have been included.

2.3 Hardware platforms examples

In this section, three examples of hardware platforms will be described. The first one is a very flexible mote that can work with different protocols networks (802.15.4, ZigBee Pro or RF) or connected directly to the Internet with a GSM/GPRS modem. It is based on a low power microcontroller with limited computing capabilities but the flexibility and ease of programming makes it different from the competitors. Another different example is a mote with a more rigid network configuration but with a more powerful microprocessor that can run not only complex control algorithms but also image processing applications. The third example is one of the few platforms that are focused on WirelessHART. In this case the motes do not have the usual array of available sensors; instead they are intended to provide wireless capability to HART compliant sensors.

2.3.1 Waspmote by Libelium

Waspmote (see figure 51) is based on a modular architecture. The idea is to integrate only the modules needed in each device. These modules can be changed and expanded according to needs. The modules available for integration in Waspmote are categorised in:

- ZigBee:/802.15.4 modules (2.4GHz, 868MHz, 900MHz). Low and high power.
- GSM/GPRS Module (Quadband: 850MHz/900MHz/1800MHz/1900MHz).

- GPS Module.
- Sensor Modules (Sensor boards).
- Storage Module: SD Memory Card.

The Waspmote is based on the Atmel ATMega1281 microcontroller running at 8 Mhz, with 128 Kb of flash RAM. This microcontroller is often used in motes and it is supported by TinyOS. It has an accelerometer and temperature on-board sensors, and different sensor boards can be added:

- **Gases Board**: Carbon Monoxide, Carbon Dioxide, Methane, Oxygen, Hydrogen, Ammonia, Isobutane, Ethanol, Toluene, Hydrogen Sulphide, Nitrogen Dioxide, atmospheric pressure, humidity and temperature.
- **Event Detection Board**: pressure, weight, curvature, stretch, vibration, impact, inclination, temperature, liquid level, light, PIR, Hall effect and presence of liquid.

Besides that sensor boards, a prototype sensor board is available to fit directly to the mote any sensor. Waspmote has also different input-output connections:

- 7 analog inputs (10 bit A/D converter).
- 8 digital input/output.
- 1 PWM output (8 bit).
- 1 I2C socket
- 2 UART.
- 1 USB.

The communication options in Waspmote are based on 802.15.4/ZigBee protocols, and different modules with different ranges can be added (see table 2). A GSM/GPRS modem from Sagem can also be added.

A very interesting option is that a SD Card of up to 2 Gb. can be used to store data from sensors, etc., or to load previously saved data. The file format is FAT16, so it is readable/writable in a conventional PC.

All the previous options can be plugged to the motherboard of the Waspmotes (see figure 52).

Model	Protocol	Frequency	txPower	Sensitivity	Range *
XBee-802.15.4	802.15.4	2.4GHz	1mW	-92dB	500m
XBee-802.15.4-Pro	802.15.4	2.4GHz	100mW	-100dBm	7000m
XBee-ZB	ZigBee-Pro	2.4GHz	2mW	-96dBm	500m
XBee-ZB-Pro	ZigBee-Pro	2.4GHz	50mW	-102dBm	7000m
XBee-868	RF	868MHz	315mW	-112dBm	40km
XBee-900	RF	900MHz	50mW	-100dBm	10km
XBee-XSC	RF	900MHz	100mW	-106dBm	24km

** Line of sight and 5dBi dipole antenna*

Table 2

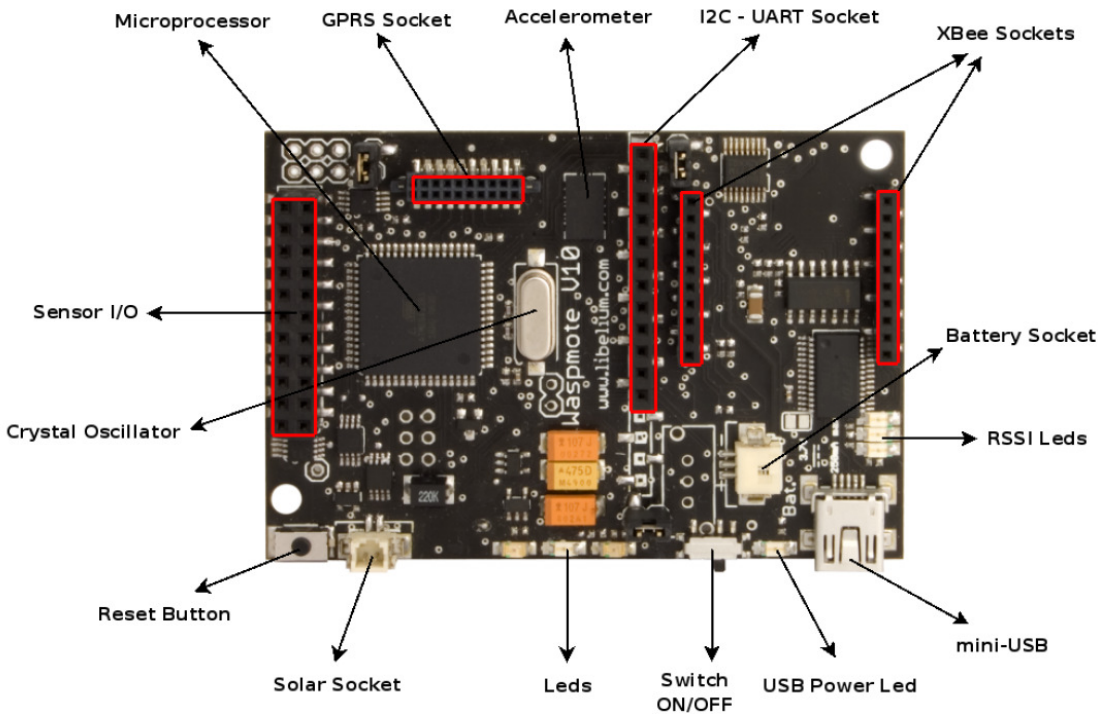


Figure 52

The power in Waspmotes comes from a 1900 mAh lithium battery that can be charged using the USB connector or from a small solar photovoltaic panel (rigid: 12 V/ 200 mA or flexible: 7V/100 mA). Power management in Waspmote is quite flexible with four different operating modes (On, Sleep, Deep-sleep and Hibernate).

The interface between the sensor network and the internet is made through a PC USB gateway or by means of a powerful and flexible router named Meshlium. Meshlium uses 5 different interfaces to connect to devices**:** WiFi, ZigBee, Bluetooth, GPRS and Ethernet. It is based on open source technologies (Linux) and it can store up to 32 Gb of data in internal databases (MySQL and Postgres). Data can also be published in Web 2.0 systems.

2.3.2 Crossbow Imote2

The **Imote2** (see figure 53) is an advanced wireless sensor node platform. It is built around the low-power PXA271 XScale processor and integrates an **802.15.4 radio** (CC2420) with a built-in 2.4GHz antenna. The design is modular and stackable with interface connectors for expansion boards on both the top and bottom sides. The top connectors provide a standard set of I/O signals for basic expansion boards. The bottom connectors provide additional high-speed interfaces for application specific I/O. A battery board supplying system power can be connected to either side.

Figure 53

The Imote2 is based on the Intel PXA271 CPU. This processor can operate in a low voltage (0.85V), low frequency (13MHz) mode, hence enabling very low power operation. The frequency can be scaled from 13MHz to 416MHz with Dynamic Voltage Scaling. This increases the computing power to a level much higher than the Waspmote, but at the cost of a much larger power requirements. If this is not a problem, then this mote is a much better alternative for complex control algorithms.

The processor has a number of different low power modes such as sleep and deep sleep. The PXA271 is a multi-chip module that includes three chips in a single package, the CPU with 256kB SRAM, 32MB SDRAM and 32MB of FLASH memory. It integrates many I/O options making it extremely flexible in supporting different sensors, A/Ds, radios, etc. These I/O features include I2C, 2 Synchronous Serial Ports (SPI) one of which is dedicated to the radio, 3 high speed UARTs,

GPIOs, SDIO, USB client and host, AC97 and I2S audio codec interfaces, a fast infrared port, PWM, a Camera Interface and a high speed bus (Mobile Scaleable Link). Note that being a much more powerful processor not only complex control algorithms can be implemented in real time, but also other applications based on image processing could be implemented.

The processor also supports numerous timers as well as a real time clock. The PXA271 includes a wireless MMX coprocessor to accelerate multimedia operations. It adds 30 new media processor (DSP) instructions, support for alignment and video operations and compatibility with Intel MMX and SSE integer instructions.

The Imote2 uses the CC2420 IEEE 802.15.4 radio transceiver from Texas Instruments. The CC2420 supports a 250kb/s data rate with 16 channels in the 2.4GHz band. The Imote2 platform integrates a 2.4GHz surface mount antenna which provides a nominal range of about 30 meters. For longer range a SMA connector can be soldered directly to the board to connect to an external antenna.

The power needs of Imote2 can be satisfied using different configurations:

- **Primary Battery:** This is typically accomplished by attaching a Crossbow Imote2 Battery Board to either the basic or advanced connectors.
- **Rechargeable Battery:** This requires a specially configured battery board attached to either the basic or advanced connectors. The Imote2 has a built-in charger for Li-Ion or Li- Poly batteries.
- **USB:** The Imote2 can be powered via the on-board mini-B USB connector. This mode can also be used to charge an attached battery.
- **Battery Pads:** A suitable primary battery or other power source can be connected via a dedicated set of solder pads on the Imote2 board.

Imote2 is based on TinyOS 1.x, and it is supported by MoteWorks, the free-download software platform of Crossbow. This software platform enables the creation of wireless sensor networks. A Moteworks wireless network deployment is composed of the three distinct software tiers:

1. The **Mote Tier**, where *XMesh* resides, is the software that runs on the cloud of sensor nodes forming a mesh network. The *XMesh* software provides the networking algorithms required to form a reliable communication backbone that connects all the nodes within the mesh cloud to the server.
2. The **Server Tier** is an always-on facility that handles translation and buffering of data coming from the wireless network and provides the bridge between the wireless Motes and the internet clients. *XServe* and *XOtap* are server tier applications that can run on a PC or Stargate.
3. The **Client Tier** provides the user visualization software and graphical interface for managing the network. Crossbow provides free client software called *MoteView*, but *XMesh* can be interfaced to custom client software as well.

MoteWorks is provided with a set of software development tools for custom Mote applications, including custom sensor board drivers, sensor signal conditioning and processing and message handlers. MoteWorks includes an optimized cross-compiler for the target mote platform and an advanced editor for TinyOS application

development. MoteWorks automatically installs and configures these development tools for quick set-up and rapid start of development.

2.3.3 SMARTMESH IA-510 WirelessHART

Dust Network SmartMesh IA-510 is one of the few t WirelessHART-compatible sensor networks. The SmartMesh IA-510 system offers industrial automation vendors an Intelligent Networking Platform that delivers dynamic network optimization and intelligent routing to achieve the carrier class data reliability, lower latency and deterministic power management required for the industrial automation market. The SmartMesh IA-510 system consists of the PM2511 embedded network manager and two mote form factors: the DN2510 Mote-on-Chip and the M2510 RF-certified mote module.

The M2510 (see figure 54) is tailored for use in battery-powered and energy-scavenging wireless devices, and is engineered for applications that demand proven performance and scalability. It has an IEEE 802.15.4-compliant design and integrated long-range signal amplification, so that it has a decade of battery life on two AA batteries. Mote current consumption is configurable, enabling power scavenging technologies (e.g. 4-20mA loop scavenging, solar cells), and it also has battery metering capability. Additionally, all motes can function as both battery-powered routers and nodes, enabling a full mesh topology that provides more redundant routes and higher network performance. The network-ready module integrates all radio circuitry components, including an MMCX-type antenna connector. The DN2510 Mote-on-Chip integrates most of the functions of the M2510 in an easy-to-integrate 12 mm x 12 mm System-in-Package (SiP) (see figure 55).

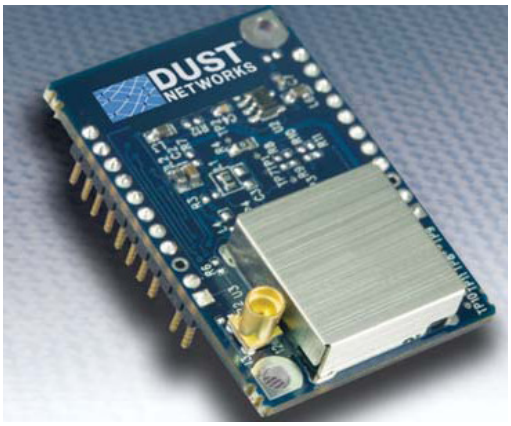


Figure 54

Figure 55

The other component of the SMARTMESH IA-510 system is the PM2511 embedded network manager (see figure 56). The PM2511 is tailored for use in line powered WirelessHART gateways and controllers, and enables the development of wireless sensor networks. The embedded network manager offers a comprehensive API to deliver rich and flexible functionality without complex coding. This API also provides full visibility and control over network configuration, security administration, network status and performance statistics.

Figure 56

3 Long-distance Communication Systems

One of the features of a distributed control system is that it is possible for some of the stations to be placed at remote locations, far from each other, where cable based communication is not possible. In this case, there are several communication systems that can be chosen to transmit the signals from the remote stations to the control centre, depending on the geographical distribution of stations, the costs and the amount of data.

The third application of WP7, Watering Channels, is an example of this kind of distributed system, where real time data collected by the sensors that are connected to the remote stations has to be sent to the control centre.

In this section, the following communication systems are described, and their advantages and disadvantages are summarized:

1. Analogical PMR
2. Analogical Trunking
3. Digital Radio Links
4. Digital Trunking: TETRA
5. GSM/GPRS
6. UMTS
7. Satellite-VSAT
8. ADSL
9. Wimax

In Figure 48, these technologies have been classified according to three parameters: velocity, mobility and application.

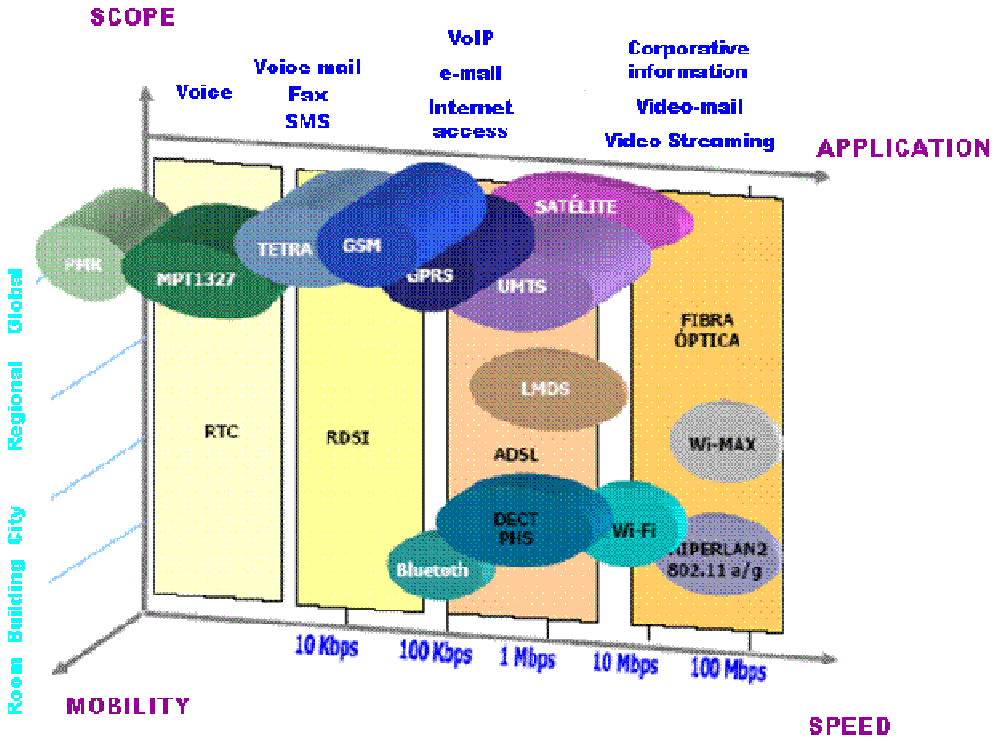


Figure 48

3.1 Analogical PMR

The most relevant characteristics of a communication system based on analogical PMR are:

- Analogical private radiotelephony systems, used traditionally for multiple applications, are normally open systems, and they can use free or licensed frequencies
- Initially these systems were mono-canal and mono-location, and have developed to multi-canal and multi-location networks
- To broaden the coverage range, some relay masts are used, made up of one or more radio stations with the possibility of interconnection
- Own infrastructure

	Advantages	Disadvantages
Analogical PMR	Simplicity	Proprietary protocols
	Low cost	Limited bandwidth
	Independence from external communication operators	Not safe
		Oriented to voice services

3.2 Analogical Trunking

Main topics of this technology:

- This technology is designed essentially for voice communication.
- Private access.
- Analogical trunking is an access technology that needs a "main" transport network that provides interconnection.
- Coverage is provided by the base stations, usually located beside the main transport network. These base stations receive data from this transport network and send it to the control points and vice versa.

	Advantages	Disadvantages
Analogical Trunking	Communications in a wide area	Oriented to voice services
	High availability	A process of frequencies assignment is necessary
	Independence from external communication operators	Low rate of data transmission (< 1200 bps)
	High flexibility	Low spectral efficiency
	Standardized and tested systems	Non-existing main communication network. High engineering and infrastructure costs
	Good coverage in extensive areas around base stations	High maintenance costs

3.3 Digital radio Links

This system is based on a high capacity network of radio links (transport infrastructure). To access the control points, another network of radio links with less capacity (connected to the main network) is used.

All the infrastructure belongs to the user, except perhaps at some points where it is impossible to install personal infrastructure and it has to be shared with others.

Radio links use digital transport technology such as **PDH** (Plesiocronus Digital Hierarchy) or **SDH** (Synchronous Digital Hierarchy), establishing the way to canalize data through the link, and the way to extract and insert the flow of data. This kind of link can work between 4GHz and 13GHz, with digital efficient modulations like 128QAM (Quadrature Amplitude Modulation).

The corresponding schema is shown in Figure 49

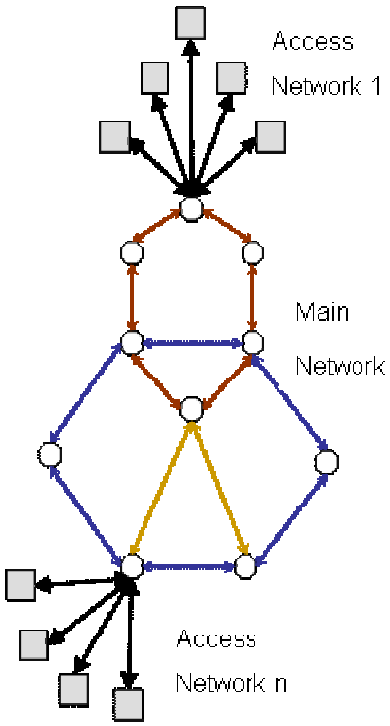


Figure 49

	Advantages	Disadvantages
Digital Radio Links	Very wide bandwidth, that integrates voice and data (and high speed video)	Direct visibility (point to point) between main radio links is required
	Very high availability	A process of frequencies assignment and licenses is necessary
	Independence from external communication operators	Non-existing main communication network. High engineering and infrastructure costs
	Scalability if well planned	High maintenance costs

3.4 Digital Trunking: TETRA

This system (Figure 50) is based on a cellular access technology but with private features. It would be an own network. It has the disadvantage that it is not a solution by itself, but needs a main transport network that provides interconnection (for example, a radio link network).

This radio link network manages the traffic in the network. Coverage is provided by the base stations, usually located beside the main transport network. These base stations receive data from this transport network and send it to the control points and vice versa.

The functioning of this technology is based on **TDMA** (Time Division Multiple Access). Thanks to this, all equipment near a base station shares the same frequency couple, one to receive and the other to transmit. To access simultaneously, the signal is divided into 4 different temporal slots, the first of them is used to control the link (call establishment, small messages …), and the rest can be used for voice or data, depending on the user's needs. If 3+1 channels are not enough in a certain place, the standard takes into account the addition of channels (scalability).

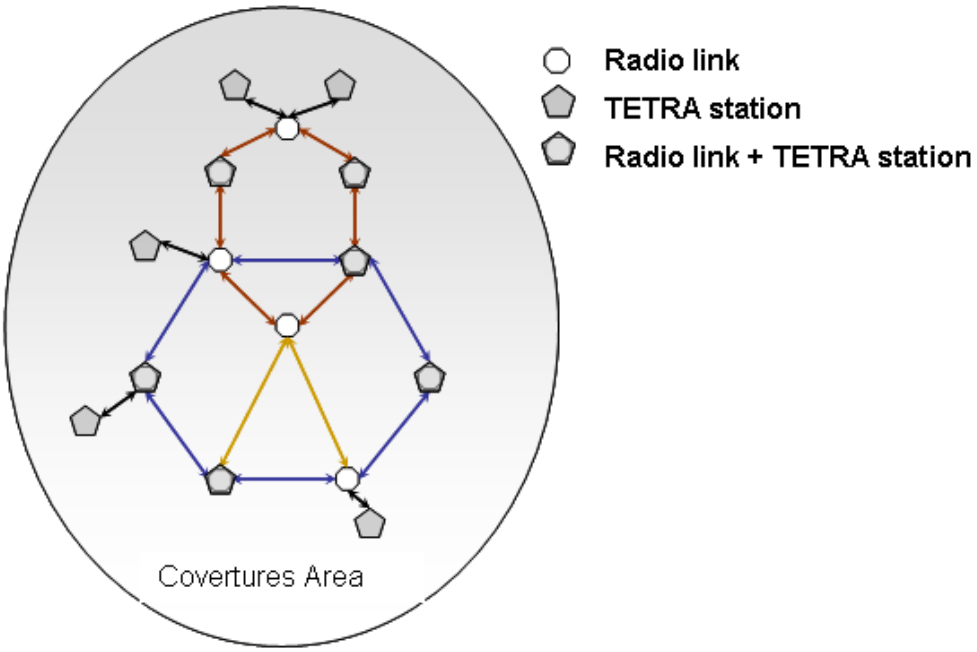


Figure 50

	Advantages	Disadvantages
Digital Trunking: TETRA	High transmission speed	Oriented to voice services
	Optimization of radioelectric spectrum: 4 channels each 25 kHz	A process of frequencies assignment is needed
	Independence from external communication operators	Non-existing network. High engineering and infrastructure costs
	Transmission of voice and data (and slow video)	High maintenance costs
	Very high flexibility, scalability and availability	Design and implementation of a transport back-bone (i.e. digital radio links)
	Provides voice services to mobile and portable equipment located in an area next to the network	
	Standardized and tested systems	

3.5 GSM/GPRS

In general, this technology is based on the use of cell phone networks and data belonging to an external operator (Figure 51). This external network is used only for exploitation needs. Some of the main features are:

- Specific modems (appropriate for each network) are needed. If necessary, connections are established point to point
- These modems include standard connection interfaces of industry (RS232 and Ethernet) for communication among data equipment (remote terminal units, PCs, ...)
- GPRS uses GSM infrastructure
- Data transmission speed via GPRS goes from 56 Kbit/sec to 114 Kbit/sec
- GPRS supports SMS, MMS, WAP, text and TCP/IP data

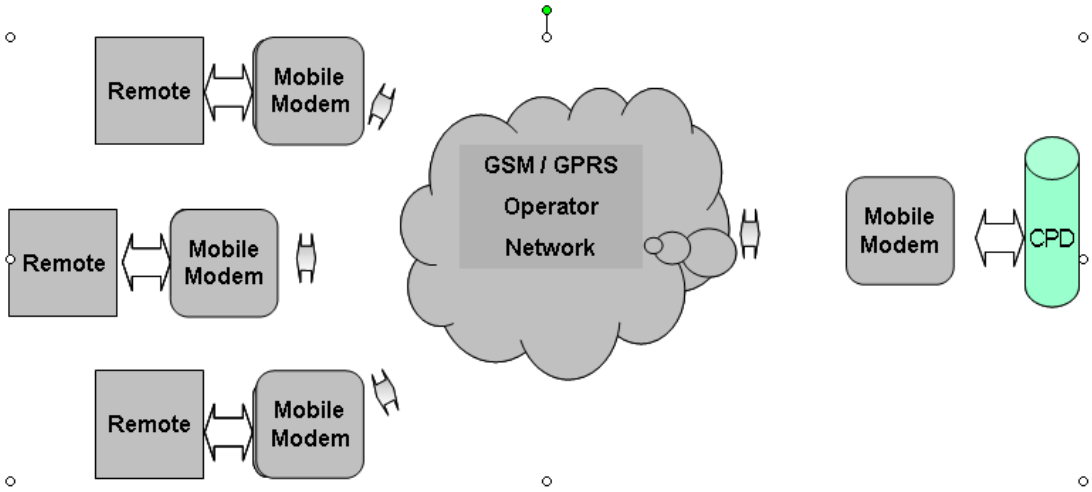


Figure 51

	Advantages	Disadvantages
GSM / GPRS	Internet access	Possibility of delays in the delivery of information
	Efficient use of radio-electric spectrum	No storage mechanisms
	All infrastructure exists and belongs to external operators	It depends on an external operator
	Transmission of voice and data (and slow video)	Narrow bandwidth
	Very high flexibility. Scalability	GPRS doesn't have coverage where GPS does
	No problems of frequency assignment	

3.6 UMTS

This technology is based on the use of cell phone networks and data belonging to an external operator. Specific modems (appropriate for each network) are needed. Data are transmitted in a 'burst' way, that is, it isn't necessary a call establishment to transmit data, it is always connected.

	Advantages	Disadvantages
UMTS	Higher transmission speed than GSM / GPRS	Dependency on an external operator
	More capacity than GPRS 7,2 (Mbit/sec)	UMTS doesn't have coverage where GPRS/GPS does. It's necessary to install new infrastructure to provide coverage
	Internet access	
	All infrastructure exists and belongs to external operators	
	Very high flexibility and scalability	
	A process of frequencies assignment is not necessary	
	Voice transmission (high quality) and data and video	

3.7 Satellite links

Satellite based Internet connections are independent of control software type, thus everything in this section can be applied to any control system. Some aspects and features to be taken into account are:

- Different Satellite links are offered for different kinds of users:
    - Individual user: lowest priority, lowest quality of service guarantee, more expensive for higher bandwidth.
    - Small and medium business and industry: better service and less expensive for higher bandwidth. Virtual Private Networks can be used.
    - Large corporations, municipalities, government, military users: best quality of service guarantee. Some service providers specialize in these kinds of users.
- Coverage: Worldwide coverage cannot be guaranteed with just one satellite. Some providers cannot use enough satellites to offer worldwide coverage.
- Bandwidth and quality of service offer.
- Cost:
    - Installation: depending on the satellite and the geographical location, the satellite dish may be larger and the equipment more expensive. In most cases VSAT dishes with a diameter of up to 2.5 m will be enough.
    - Use and maintenance: cost is variable depending on the service provider, bandwidth and guaranteed quality of service.
- Types of satellite links:
    - Unidirectional: There is an emitter and several receptors (conventional TV Satellite dishes).
    - Hybrid Bidirectional: The download is through a satellite link, but outgoing traffic goes over a different connection like a modem over a phone link. This is used only when the outgoing traffic is very small.
    - Bidirectional: This is the best type for distributed control systems and uses the satellite link for both incoming and outgoing traffic. Usually the transmission and reception speeds are different (asymmetric speeds) and can support virtual private networks.

	Advantages	Disadvantages
Satellite	Very high flexibility and scalability	Dependence on an external operator and high renting costs
	Very low maintenance costs and engineering costs	Problems of prioritization if the bandwidth is saturated
	No problems of poor coverage	High latencies (around 1000 ms)
	All infrastructure exists and belongs to external operators	High cost of equipment for non critical control points
	It requires little infrastructure, because: - there are no radio links or relay masts	Voice services to mobile and portable equipment located in an area near to the network is not provided
	A process of frequency assignment is not necessary	
	Transmission of voice, data and video	

3.7.1 Some examples of satellite links and service providers

Mobile access with BGAN (Broadband Global Area Network): This is a network suited to mobile and temporal applications. It is based on INMARSAT satellites, and there are different service providers that allow for connection to BGAN. The bandwidth is limited to 0.5 Mbps (but only 0.25 Mbps are guaranteed). Furthermore, the BGAN antenna is flat and very small (see Figure 52).

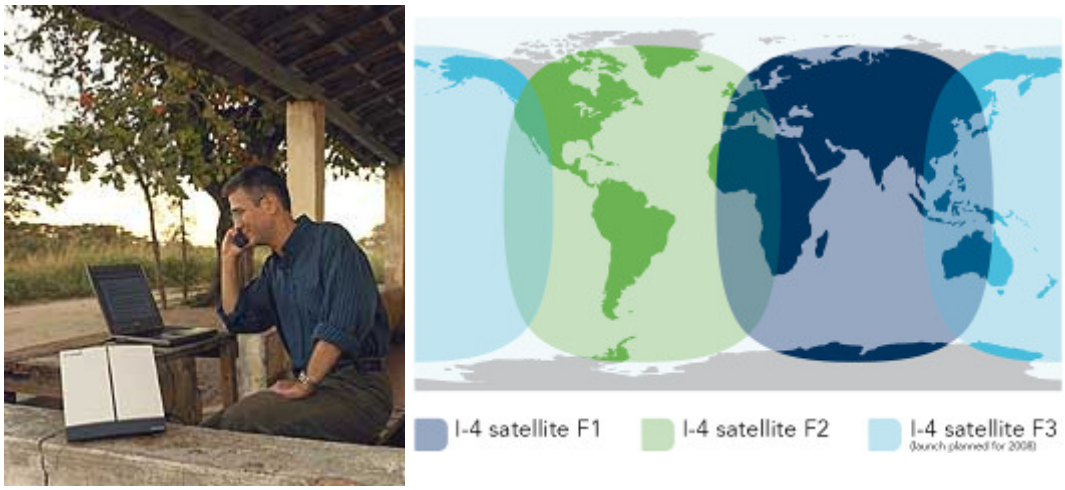


Figure 52

A great advantage of BGAN is its worldwide coverage (see Figure 52). Voice over the satellite link is also supported. However it can be very expensive (up to 6450 Euros monthly for 2000 Mb of traffic).

Access using a fixed VSAT satellite dish: VSAT dishes are quite small (diameter up to 2.5 meters, see Figure 53) and offer access to different service providers. Bandwidth is usually between 2 and 4 Mbps, but the offer depends on which service provider is chosen.

Figure 53

Nowadays, the user can choose from different service providers. SatConxion uses the Eutelsat satellite and offers 2/1 Mbps at 722 € monthly. There are service providers specializing in large users like Tachyon with access from Europe, the Middle East and the Americas and up to 8 Mbps with a guarantee of service quality. Another example is PCCW GLOBAL, with 4 Mbps and guaranteed quality of service. It uses different satellites and transmission bands to offer access in Europe, Africa, Asia and Oceania (see Figure 54).

T – 10 C Band | T – 18 Ku Band | NSS-6 Ku Band Middle East Beam | NSS-6 Ku Band SE Asia Beam

Figure 54

3.8 ADSL

The main features are:

- Asymmetric digital client line technology
- Cable communication technology, which uses the commuted telephone network
- Signals are treated digitally, getting high transmission speed and using all the available capacity
- The treatment of voice and data is different (using divisors)

	Advantages	Disadvantages
ADSL	Very efficient use of radio electric spectrum	Dependence on an external operator. Renting costs
	Very low maintenance costs	Voice services to mobile and portable equipment located in an area near to the network are not provided
	High speed	ADSL is not worldwide
	High transmission speed of audio and video	
	Plug and play: easy to install and integrate	
	Internet access	

3.9 Wi-max

This technology is characterized by:

- Medium-range broadband Wireless technology (maximum 15 km), that uses the 5.4 GHz band.
- Technology OFDM is used (Orthogonal Frequency Division Multiplex). Thanks to this, it is possible to reach 15 km, taking advantage of signal rebounds
- It is possible to reach 50 Mbps
- Two possibilities of configuration: point to point and point to multipoint. In the last option a central node provides coverage to the rest of the points, which use this main node to communicate with the rest
- If necessary some intermediate relay masts can be used.

	Advantages	Disadvantages
Wi-max	High transmission speed and wide bandwidth	High initial investment
	Good coverage	Direct sight between points is necessary
	Independence from external communication operators, long-range	It is not useful if distances are greater than 15 km
	Quick installation	
	Very high flexibility and scalability	
	Low maintenance, engineering and infrastructure costs	

4 References

[1] Infusion Overview Brochure, Invensys PLC, available at:
http://ips.invensys.com/en/products/entcontrol/Documents/InFusion%20Overview%20Brochure.pdf

[2] Infusion Condition Manager Datasheet, Invensys PLC, available at:
http://ips.invensys.com/en/products/assetmanage/Documents/InfusionConditionMgr.pdf

[3] Infusion View Datasheet, Invensys PLC, available at:
http://ips.invensys.com/en/products/entcontrol/Documents/InFusionView.pdf

[4] Infusion Access Datasheet, Invensys PLC, available at:
http://ips.invensys.com/en/products/entcontrol/Documents/InFusionAccess.pdf

[5] The Mesh Network Control Architecture, Invensys PLC, available at:
http://resource.invensys.com/iaseries/pss/21h7/21h7c2b3.pdf

[6] The MESH Control Network Ethernet Equipment, Invensys PLC, available at:
http://resource.invensys.com/iaseries/pss/21h7/21h7c3b4.pdf

[7] Experion HS Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/4EB9E2F5-E541-4346-82D0-071986655719/75015/ExperionHS_PIN_March09.pdf

[8] Experion Vista Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/E7B2D684-6C50-4C6E-BA3A-66A64B779A22/60243/ExperionVistaPIN_Aug08_PN0722.pdf

[9] Fault Tolerant Ethernet Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/329EF29C-7DA7-40DF-819C-094DC22FFCA3/66967/FTE_PIN_06.pdf

[10] Digital Video Manager Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/7B22FB82-5574-45C3-8E8A-F3606F76B095/63660/DVM_PIN_June2008.pdf

[11] Uniformance Process Studio Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/B21A95CA-EAC5-4C48-9CD2-3584BB2B72A0/62138/Uniformance_Process_Studio_PIN.pdf

[12] Experion eServer Product Information Note, Honeywell, available at:
http://hpsweb.honeywell.com/NR/rdonlyres/D82150AB-AA37-4C57-87B8-78C089AFAF12/81418/eServerPIN_Aug09_eop.pdf

[13] Industrial IT System 800xA Brochure, ABB, available at:
http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/863e0a1b1b8e786dc12576af005e9411/$File/3BUS095061_L_en_Industrial_IT_System_800xA_Brochure.pdf

[14] System 800xA 5.0 Control and I/O Overview, ABB, available at:
http://www05.abb.com/global/scot/scot313.nsf/veritydisplay/759fb84f9f6786f8c125758d0059bd44/$File/3BSE047351_C_en_System_800xA_5.0_Control_and_I_O_Overview.pdf

[15] System 800xA 5.0 Engineering Overview, ABB, available at:
http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/77fe6402f663a7f2c125721e0078a40a/$File/3BDD013082_H_B_en_System_800xA_5.0_Engineering_Overview.pdf

[16] System 800xA Engineering Overview: Process Control Equipment Library, ABB, available at:
http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/fe4e401880306efec1256f9e000174e7/$File/3BUS092091R0001_H_en_System_800xA_Engineering_Overview___Process_Control_Equipment_Library__high_resolution.pdf

[17] System 800xA 5.0 Asset Optimization Overview, ABB, available at:
http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/f2406220ee881771c12574b40076ab32/$File/3BUS094382_H_B_en_System_800xA_5.0_Asset_Optimization_Overview_hires.pdf

[18] Vijeo Citect Technical Overview, Schneider Electric, available at:
http://www.global-download.schneider-electric.com/852575A6007E5FD3/all/BEEFC5BA1933A2228525760E0069635E/$File/dia6ed1090808en.pdf

[19] Vijeo Terminal Services, Schneider Electric, available at:
http://www.global-download.schneider-electric.com/852575620060EED7/all/C125713F005265E2C125756700506F85/$File/vijeo%20terminal%20services_lo%20res.pdf

[20] Vijeo Citect technical brochure, available at:
http://www.global-download.schneider-electric.com/85257578007E5C8A/all/9F26870B85D643D088257578005E232D/$File/dia5ed1070608en.pdf

[21] Simatic WinCC brochure, Siemens, available at:
http://www.automation.siemens.com/salesmaterial-as/brochure/en/brochure_simatic-wincc_en.pdf

[22] Simatic Plant Intelligence, Siemens, available at:
http://www.automation.siemens.com/salesmaterial-as/brochure/en/brochure_plant-intelligence_en.pdf

[23] Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches, V. C. Gungor,and G. P. Hancke, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 10, OCTOBER 2009, pp. 4258-4265.

[24] Which Wireless Technology for Industrial Wireless Sensor Networks? The development of OCARI Technology, K.A.l Agha, M.H. Bertin, T. Dang, A. Guitton, P. Minet, T. Va, and J.B. Viollet, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 10, OCTOBER 2009, pp. 4266-4278.

[25] System Architecture Directions for Networked Sensors, J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. S. J. Pister,i n Architectural Support for Programming Languages and Operating Systems, pages 93–104, 2000.

[26]The nesc language: A holistic approach to networked embedded systems, D. Gay, P.Levis, R. Behren, M. Welsh, E. Brewer, and D. Culler, iIn Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation (PLDI), pages 1–11, New York, NY, USA, 2003. ACM Press.

[27] Flexible hardware abstraction of the TI msp430 microcontroller in tinyos, V. Handziski, J. Polastre, J. H. Hauer, and C. Sharp, in Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys), pages 277–278, Baltimore, MD, USA, November 2004. ACM Press.

[28] The emergence of networking abstractions and techniques in tinyos, P. Levis, S. Madden, D. Gay, J. Polastre, R. Szewczyk, A. Woo, E. Brewer, and D. Culler, in Proceedings of the First USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI 2004), San Francisco, California, USA, mar 2004.

[29] TinyOS 1.x Tutorial, available at: http://www.tinyos.net/tinyos-1.x/doc/tutorial/.

[30] TinyOS Programming, P. Levis and D. Gay, Cambridge University Press, 2009.

[31] T2: A second generation os for embedded sensor networks, P. Levis, D. Gay, V. Handziski, J.-H.Hauer, B.Greenstein, M.Turon, J.Hui, K.Klues, C.Sharp, R.Szewczyk, J.Polastre, P.Buonadonna, L.Nachman, G.Tolle, D.Culler, and A.Wolisz, Technical Report TKN-05-007, Telecommunication Networks Group, Technische Universität Berlin, November 2005.

[32] Flexible hardware abstraction for wireless sensor networks, V. Handziski, J. Polastre, J.-H. Hauer, C. Sharp, A. Wolisz, and D. Culler, In Proceedings of Second European Workshop on Wireless Sensor Networks (EWSN 2005), Istanbul, Turkey, February 2005.

[33] T2: What the second generation holds, P. Levis *et al.*, available at: http://csl.stanford.edu/~pal/talks/berkeley-seminar-05.pdf