Remote Supervisory Control and Data Acquisition System for Palm Diesel Pilot Plant

Andrew Yap Kian Chung*

ABSTRACT

The enormous growth of the Internet in recent years have made significant impact on industrial development. Browser applications with graphical user interfaces have made accessing and navigating the web across geographical borders very easy. One such application is remote supervisory control and data acquisition (R-SCADA). Its objective is to implement a totally integrated automation (TIA) approach on the palm diesel pilot plant via information technology (IT) on a publish-subscribe and event-driven basis using Terminal Control Protocol/Internet Protocol (TCP/IP). The WinCC Server and WinCC Web Navigator Server used in the system are separated from the communication via a channel structure. The advantages of R-SCADA are its capability to operate and monitor over long distance, remote diagnostics and fault elimination, rapid update rates due to event-driven communication, integration of management and diagnostic clients that have access to current production data and high safety security standard. Even though data is exposed to certain risk, there are several important concepts regarding a secure transaction. This approach can be easily implemented in a palm oil mill or a refinery.

INTRODUCTION

The process flow diagram of the palm diesel pilot plant in MPOB is shown in *Figure 1*. Generally, the process can be divided into three stages (Cheah *et al.*, 1998):

- esterification of the free fatty acids present in the crude palm oil into methyl esters using solid acidic catalyst at a temperature of 80°C and pressure of 3 kg cm^{-2} as shown in the reaction equation (1).

$$RCOOH + CH_3OH \rightleftharpoons RCOOCH_3 + H_2O \quad (1)$$

- transesterification of the triglycerides into methyl esters using sodium methoxide, $NaOCH_3$, as the catalyst with excessive methanol as shown in reaction equation (2).

$$(CH_2\text{-}O\text{-}COR)_2CH\text{-}O\text{-}COR + 3CH_3OH \rightarrow 3RCOOCH_3 + C_3H_5(OH)_3 \quad (2)$$

- product separation and purification involving the separation of methyl esters, methanol and glycerol, and the washing of esters to remove traces of impurities. Emulsion is easily formed during the washing step and sodium chloride (NaCl) is used to break the emulsion. The washed esters are then dried in a vacuum dryer.

The control objectives are:

- the free fatty acids, FFA, content of the oil to be reduced to less than 0.5% after the esterification process;

* *Malaysian Palm Oil Board, P. O. Box 10620, 50720 Kuala Lumpur, Malaysia.*

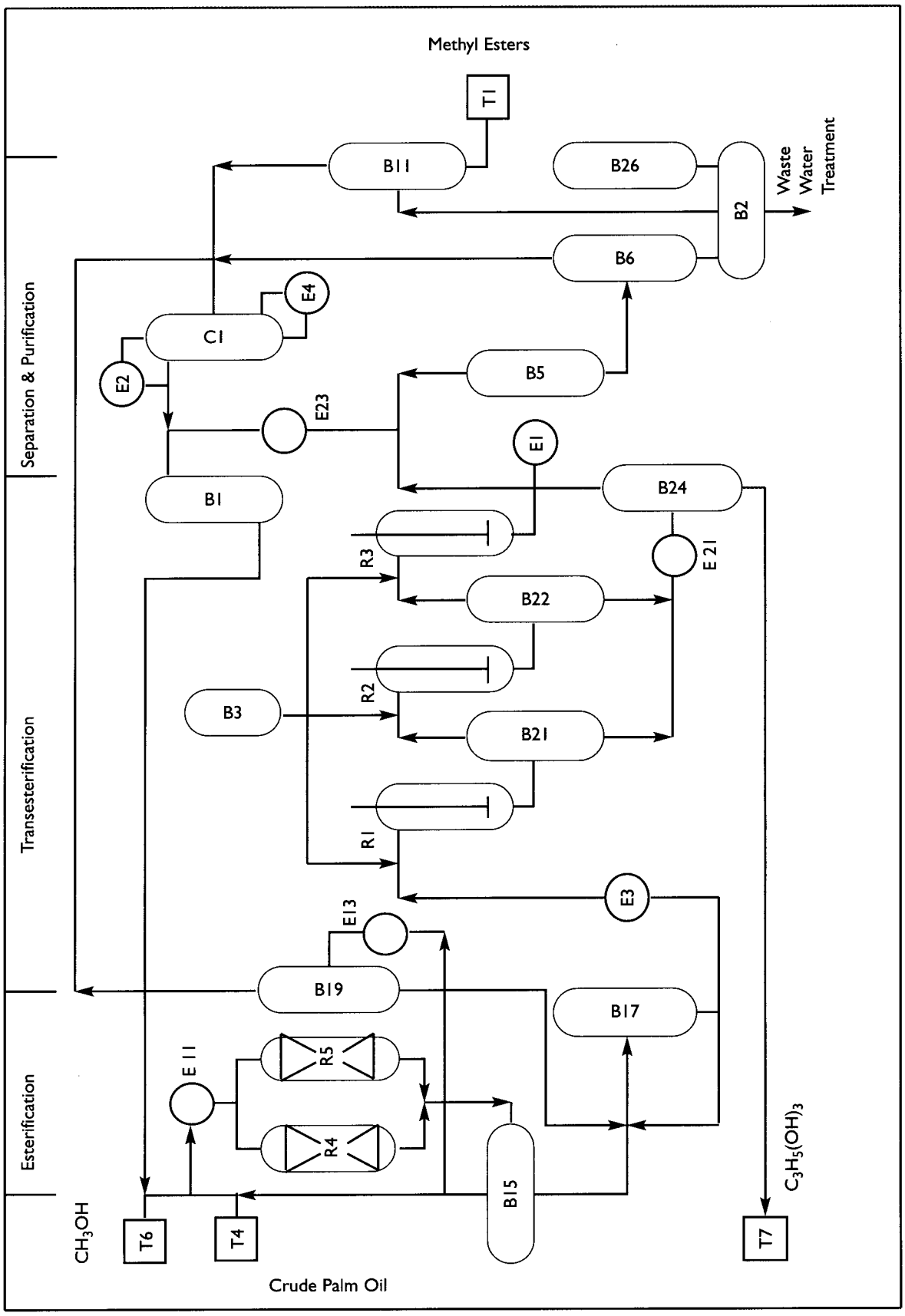

Figure 1. Palm diesel pilot plant process flow diagram.

- the conversion of the transesterification process to exceed 98%; and
- minimum soap forming.

A Siemens SIMATIC S7-300 system used in the palm diesel pilot plant was merely controlled directly without any online optimization. All the set points of the controllers were determined manually. The control system consisted of analogue input-output modules, which were operated using 4 to 20 mA signals, and digital input-output modules, which were operated using 24 Vdc signals. The communication between the central processing unit, CPU, and the control modules used the PROFIBUS protocol. Windows Control Center (WinCC) running under NT platforms was used as the Human Machine Interface (HMI) to observe the pilot plant process. The observation system is generally referred to as supervisory control and data acquisition, SCADA.

PROFIBUS is an open fieldbus with a large installed base, which can be used in a wide range of applications. PROFIBUS defines the technical and functional features of a serial fieldbus system with which distributed field automation devices can be networked in the lower to medium level performance range (Siemens, 2001).

SCADA is not a full control system but rather focuses on the supervisory level. It is purely a software package that is positioned on top of the hardware to which it is interfaced via programmable logic controllers, PLC (Daneel and Salter, 2000).

Totally Integrated Automation (TIA) stands for a revolutionary new way of combining the worlds of production and process technology. All hardware and software components are integrated in a single system. Such complete continuity is made possible through three-fold integration, which is data management, configuration and programming, and communication.

Information technology (IT) is used today in all areas. The constantly expanding range of new IT has resulted in its more frequent implementation in industrial automation (Siemens, 2001).

The objective of R-SCADA was to implement the TIA approach on the palm diesel pilot plant via IT on a publish-subscribe and event-driven basis using Terminal Control Protocol/ Internet Protocol (TCP/IP).

METHODOLOGY

The enormous growth of the Internet in recent years have made a significant impact on industrial development. One of the key factors responsible for the Internet boom was the development of the World Wide Web (www) Internet service. Browser applications with graphical user interfaces make accessing and navigating the web easy: clicking a mouse button is all that is needed to cross geographical borders (Siemens, 2000a). The specification requirements for the system are stated below.

WinCC Web Navigator Client should be operated under Windows 98 or higher, Windows ME, Windows NT 4.0 or higher, or Windows 2000 complete with Internet Explorer V5.01 or higher. There is no special hardware required; however, the IE V5.01 must be able to run and access the Intranet/Internet.

WinCC Web Navigator Server should be operated under Windows NT 4.0 and Service Pack 6a or higher, Windows 2000 SP2 with Hotfix Q300972, complete with Internet Explorer V5.01 or higher, Windows NT 4.0 Option Pack (only under Windows NT), WinCC Basic System V5.1 or higher. The minimum hardware requirements are Intel Pentium II 333 MHz, 128 MB RAM, 500 MB available Hard Drive Space and network interfaces. No license is required for the WinCC Web Navigator Client.

If Intranet information needs to be published, a network-capable computer as well as a local area network (LAN) connection and a system that breaks up computer names into Internet protocol (IP) addresses is required. This is not mandatory, but it allows users to use aliases instead of IP addresses when connecting to the server.

If the Internet information needs to be published, an Internet connection and an IP address information from an Internet service

provider (ISP), a network card that is suitable for connecting to the Internet and a domain name system (DNS) registration for the IP address is required. This is not mandatory, but it allows users to use aliases instead of IP addresses when connecting to the server.

As a prerequisite for the WinCC basic system, the WinCC RT basic license is required. No WinCC server license is required; if no local WinCC clients are operated. Without a license, the WinCC Web Navigator Server will run in demo mode for 30 days. For the permanent use of the WinCC Web Navigator Server, a license is required. Licenses are available for 3, 10, 25 or 50 clients that can simultaneously access the web server.

Before WinCC Web Server is connected to the Intranet or Internet, a concept which takes into consideration relevant security and system issues needs to be established. There are three possible approaches as stated below.

Island Solution

The Web Clients are not connected to the Intranet, but are rather used only to operate and observe the running of WinCC project. In this way, computer stations which can, for example, be used for monitoring or maintenance are set up economically.

Navigator Server on the WinCC Server

The WinCC Server and the server components of the WinCC Web Navigator are installed in one computer. The WinCC Web Navigator client can be used to operate and/or observe the running of WinCC project over both the Intranet and Internet. A client/server system can be expanded through the use of WinCC Web Navigator Clients. Firewalls are used to protect against attacks from the Internet. The first firewall protects the WinCC Web Navigator Server from attacks originating in the Internet; the second firewall provides additional protection for the intranet.

Separation of WinCC Server and WinCC Web Navigator Server

There are two possible communications using this concept as stated below:

Communication via a channel. The WinCC Server is assigned as a group of automation devices. The project is composed as of all data, including programs, configuration data and other settings. The WinCC project is mirrored 1:1 on the computer with the WinCC Server and WinCC Web Navigator Server and is not connected to the automation devices. Data matching is performed via the (Object Linking and Embedding) OLE Process Control (OPC) channel. The WinCC Web Navigator Server requires for this purpose a license for the number of OPC tags. Two firewalls are used here as well to protect the system from unauthorized access. The first firewall protects the WinCC Web Navigator server from attacks originating in the Internet; the second firewall provides additional protection for the intranet.

Communication via the process bus. Two firewalls are used to protect the system from unauthorized access. The WinCC project is mirrored 1:1 on the computer with the WinCC Server and WinCC Web Navigator Server. Data matching is performed via the process bus.

The R-SCADA system for palm diesel pilot plant uses Separation of WinCC Server and WinCC Web Navigator Server with communication via a channel. *Figure 2* shows the system schematic drawing of the R-SCADA. WinCC/ Web Navigator is used to enable visualization and operation of the pilot plant via the Internet or Intranet. A Web Navigator Server on which the SIMATIC WinCC software is installed as the server version and a Web Navigator Client which is a thin client make possible monitoring of an ongoing WinCC project by means of an Internet browser with ActiveX support without need to have the WinCC basic system on that computer. Authorized remote clients are unable to alter the operation parameters via R-SCADA for plant security purposes. Due to the license constraint, only three clients can be served at once. User name and password are used for identification.

WinCC web configurator wizard was used to set-up and configure a WinCC/Web Navigator Server. The WinCC process picture is created

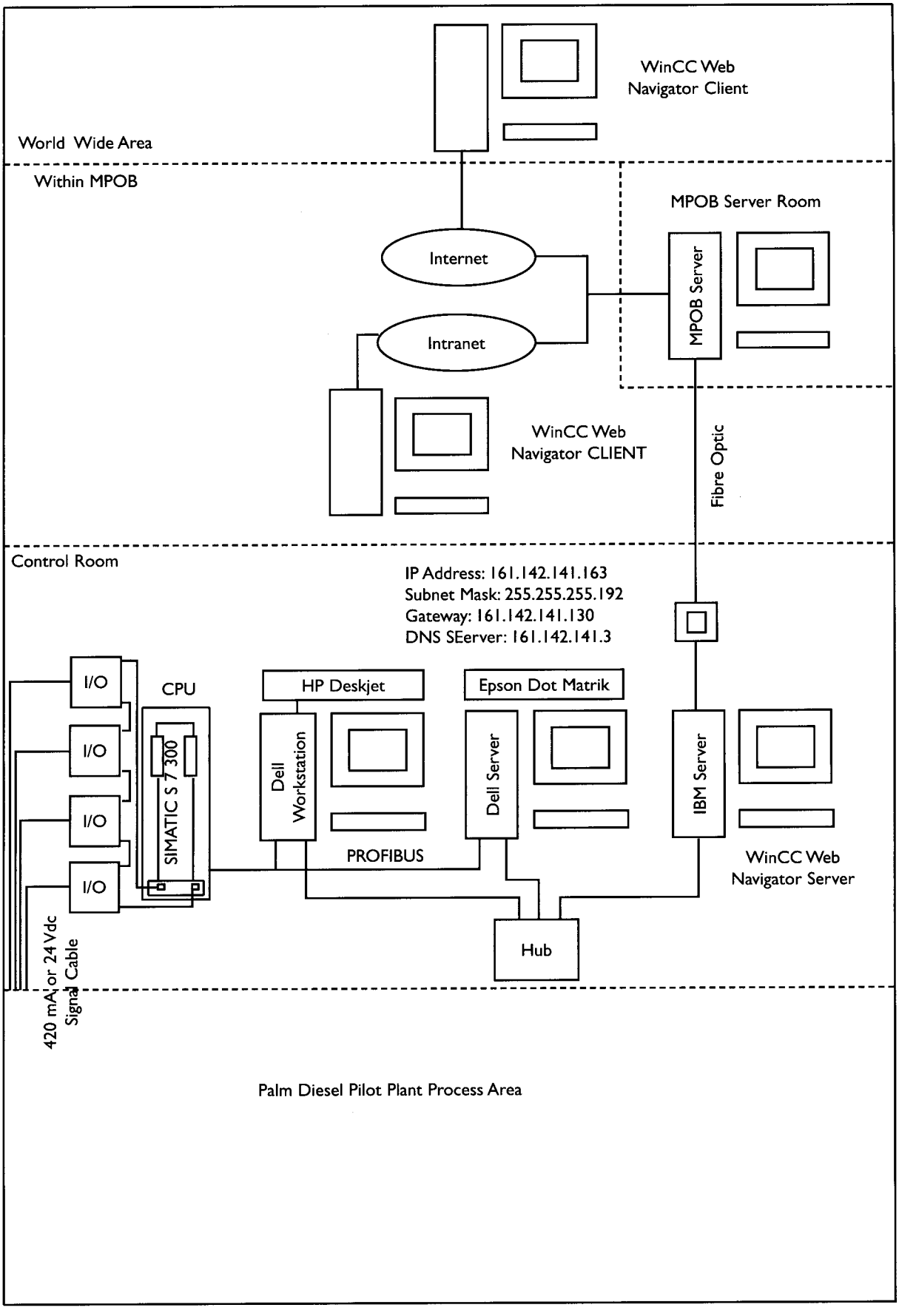

Figure 2. R-SCADA System schematic drawing.

using a WinCC Graphics Designer. The WinCC Web Publishing Wizard optimizes the picture for transfer to and representation on the Internet.

DISCUSSION

The advantages of the R-SCADA are its capability to:

- operate and monitor over long distance;
- conduct remote diagnostics and fault elimination;
- rapidly update rates due to event-driven communication;
- provide integration of management and diagnostic clients that have access to current production data; and
- provide high safety security standard.

At present, when the WinCC Web Navigator Server is connected to another computer, the data is exposed to certain risks. How the connection established plays no role, *e.g.* a connection via a local network (LAN) or a dial-up connection via an Internet provider. Unauthorized persons can have access to the data. Transmissions can be intercepted, manipulated and misdirected. By providing certain directories in the system with special security layers, the transmission of information can be controlled.

There are several important concepts for a secure transaction. Windows NT makes available powerful security functions which can be used to check users for access and monitoring. The WinCC Web Navigator Server, which is based on the Internet information servers (IIS), makes use of these Windows NT capabilities to provide security for its Internet-based services. Windows NT uses a security model which manages the security for all services through the use of a single registration process. By creating user accounts and by setting up access authorizations for these accounts, the administrators can control which resources and services are available to the users. The central administration for the WinCC Web Navigator Server is performed via the WinCC Web Administrator. In addition, the WinCC Web Navigator Server supports firewall technology. With the help of a firewall, unauthorized access can be prohibited (Siemens, 2000b).

Firewalls require the user to constantly identify himself. This identification can be performed with the aid of company-approved IP addresses, by using user-IDs and passwords - even secure ID cards and encrypted access passwords which are changed at set intervals. The most important components for the security of the WinCC Web Navigator Server are Secure Socket Layer (SSL), secure http (https), WinCC Web Administrator, firewall and secure ID card.

SSL is a protocol which guarantees the data security between http and TCP/IP. The standard for the security of www browsers and servers is defined by the World Wide Web Consortium (W3C). The W3C was established to create standard normatives for the www. Additional information can be found in the Internet under http://www.w3c.org. The SSL performs a security check before a TCP/IP connection is established. This check determines the security level which the client and the server have agreed and, over it, the necessary authenticity operations for the connection. SSL performs the encryption and decryption of the data stream of the used protocol (*e.g.* Hyper Text Transfer Protocol, http) as long as the connection exists. All information, requests as well as responses, are encrypted. This includes the information used for the authenticity check of the http access (user name/password) and all the data transferred from the server to the client. In order to use SSL, the system operator is required to provide a certificate from a certification provider, *e.g.* VeriSign. Requests for a VeriSign certificate for the Microsoft Server can be found at http://www.verisign.com.

The https is an extension of the http protocol. The SSL protocol is used to establish a secure connection between two computers, while https sends individual messages securely. The communication between the WinCC Web Navigator Server and Client is performed here using the http protocol.

A firewall is a system consisting of hardware and software that is installed at a point between two networks to only let through authorized communication traffic. Improper actions are rejected and detected unauthorized use can be recorded. Thus, firewall systems are suitable for enforcing defined rules on security (security policy). Firewalls are often used when connecting to the Internet, protecting the internal network from the dangers of the Internet. Among others, there are the following types of firewalls:

A filter firewall controls the data stream based on the data package's origin, destination, port and package type information. This information is contained in every data package. Only selected network traffic can pass through the firewall. Package filters are IT systems with special software that filters the information (IP packages) on the transport layer, *i.e.* they either let the information through or intercept it according to defined rules. The rules can operate by means of the source or target address as well as the source or destination port typical of the respective Internet service. Many routers can also be employed as package filters. Unlike static package filters, dynamic package filters do not possess a defined set of rules; instead, the firewall modifies the filter in response to certain events.

Proxy servers permit indirect access to the Internet through the firewall. A proxy is an application for network services that is executed depending on the communication of the service and from system to system. The service program of the user does not communicate directly with the target system, but with the proxy server of the firewall. The proxy evaluates the request and determines whether to establish or deny the connection. Proxy servers provide user authentication and integrity during the transfer of data between client and server. The hypertext transfer protocol (http) proxy intercepts connections from every web browser and directs the requests to the configured web server. Proxy servers support content filtering. With content filtering, only certain contents of HTML pages are permitted. In this case, the communication is rerouted via a defined port to an IP address such as the address of the WinCC server. If content filtering is active, the Web Navigator communications will no longer function. In this case, the use of SSL is recommended (Siemens, 2000c).

CONCLUSION

The advancement of IT has enabled remote supervisory control and data acquisition, which bring enormous benefits to processing industry. Even though the data is exposed to certain risks, there are several important concepts regarding a secure transaction. The separation of WinCC Server and WinCC Web Navigator Server with Communication via a channel approach used in the palm diesel pilot plant protects the WinCC Web Navigator server from attacks originating in the Internet and intranet. Thus, the data and control are secure from unauthorized access, interception, manipulation and misdirection.

REFERENCES

CHEAH, K Y; CHOO, Y M; MA, A N and YUSOF BASIRON (1998). Production technology of palm diesel. *Proc. of the 1998 PORIM International Biofuel and Lubricant Conference.* MPOB, Bangi.

DANEELS, A and SALTER, W (2000). What is SCADA? *CERN-CNL-2000-003 Vol. XXXV Issue No. 3.*

SIEMENS (2000a). *SIMATIC S7-300 – The Modular Mini PLC.* Siemens Aktiengesellschaft, Germany.

SIEMENS (2000b). *Siemens Take You to a Whole New Level in Control Software WinCC Integrated HMI.* Siemens Aktiengesellschaft, Germany.

SIEMENS (2000c). *WinCC Web Navigator - Printout of the Online Help A5E00150615.* Siemens Aktiengesellschaft, Germany.

SIEMENS (2001d). *SIMATIC WinCC Options for Modular Expansions.* Siemens Aktiengesellschaft, Germany.