IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. III (Jan - Feb. 2015), PP 37-48
www.iosrjournals.org

A Proposed Cost Effective Prototype Model for PLC Based GSM Remote Control in Home and Industrial Automation

Sherif Kamel Hussein
Department of Communications and Electronics ,October University for Modern Sciences and Arts, Giza – Egypt

Abstract: *Nowadays, wide range of sectors within a community is focusing on the usage of different communication systems to support mobile applications such as, home and industry ensuring the real-time, safe and secure behavior of these systems. Such trends merging mobile value added services and home/industrial automation technologies. This research investigates the potential for remote controlled operation of both home and industrial automation systems. The proposed model for designing this system is to develop and implement an efficient low cost PLC (Programmable Logic Control) based GSM Control module that will integrate the mobile application platforms and home/industrial automation technologies with different options of communication protocols and command structure from a cellular phone over the GSM network or internet accessing mobile home/industrial automation service and the relevant controlled devices.*

Keywords and Abbreviations: *Programmable Logic Controller (PLC) ,Micro Controller, Global System Mobile (GSM), General Packet Radio Service (GPRS), Supervisory Control and Data Acquisition System (SCADA). Attention Command (AT), Protocol Description Unit (PDU), Central Processing Unit (CPU),Short Message Service (SMS), Input/output (I/O).*

I. Introduction

People in the new era of modern science need the real-time information whenever they desire. Such technical development can be achieved through the contributions of different technological advancement of communication systems. Introduction of GSM mobile phone is one of them which is easily available, accessible, portable, cost-effective and have device availability throughout the country and the world. Hence, the idea of introducing SMS should be an efficient real-time approach in any kind of appliance control [1, 2].

Mobile phones are getting more advanced that allow researchers to develop different applications due to their ability to do almost all whatever computers can do. Remote management and control of devices is one of the areas where an application can be developed to enhance life quality. Different approaches can be followed to develop remote management or control systems, such as the use DTMF (Dual Tone Multi Frequency) technology which involves the use of mobile phones tone to perform an action, while others use Short Message Service (SMS)technology to send the command for a particular action [3]. In addition to the use of GPRS (General Packet Radio Service) technology to directly interface mobile phone with computers over communication protocols.

Supervisory control and data acquisition (SCADA) is used to describe a system where both data acquisition and supervisory control are performed. Mobile Supervisory Control and Data Acquisition (referred to as Mobile SCADA) is the use of SCADA with the mobile phone network. GSM is a wireless communication technology; most popular today for transmitting data anywhere in the world through SMS with the help of mobile phones [4, 5].

Present basis of knowledge management is the efficient share of information. The challenges that modern industrial processes have to face are multimedia information gathering and system integration. Driven by a notable commercial interest, wireless networks like GSM or IEEE 802.11 are now the focus of home security and industrial attention, because they provide numerous benefits, such as low cost, fast deployment and the ability to develop new applications. However, wireless networks must satisfy industrial requisites: scalability, flexibility, high availability, immunity to interference, security and many other that are crucial in hazardous and noisy environments.

In this paper a proposed Model is used to develop and implement low cost PLC based GSM control module as an integration of mobile application platforms and home/industrial automation technologies. In the following sections , the concept of GSM technology and the structure of integrating this technology with the micro controller and PLC systems will be introduced. An overview on the Attention (AT) and Protocol Description Unit (PDU) commands used in GSM based remote control system will be mentioned. Mobile SCADA system will be discussed and finally a proposed siemens based model will be introduced as a low cost effective integration for home/industry remote and monitoring control system.

1.1. Programmable Logic Controller (PLC) Based GSM Remote Control

A Programmable Logic Controller (PLC) is a microprocessor based control system that can be programmed to sense, activate and control industrial equipment and therefore incorporates a number of input/output terminals for interfacing to an industrial process. A control program stored in the PLC memory determines the relationship between the inputs and the outputs of the PLC. PLCs are intelligent automation stations that possess highly useful and desirable features such as [3]:

- Robustness.
- High degree of scalability: modern PLC families have a wide spectrum of CPU types that allows easy scalability in functionality and performance.
- Extensibility: the modular design of PLCs enables the extension with a wide range of digital and analog Input / Output (I/O) modules. Also, various integrated technology modules are available for various application areas.
- Sophisticated communication capabilities: modern PLCs have communication ports that provide for centralized or distributed connectivity.
- Powerful development environment: modern PLC families come with a cross development environment that support different languages for programmability, allows semi graphical hardware configuration and offer strong debugging mechanisms.

Remote access to control and monitor various devices in an industrial setting is of value to engineers and automation facilities. Current implementations of remote PLC monitor and control use dedicated PCs or web servers connected to the PLC. Figure 1 illustrates a common architecture used in industry. As shown, PLCs are connected to the network through a computer. The PLC system is usually interfaced with this computer using the serial Port or Profibus.

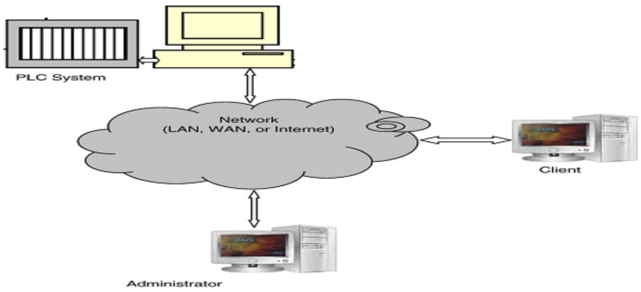

Figure1. PC-based remote accessibility

In recent years, and due to the ever increasing capabilities of PC computing and the influx of network protocols and standards, there has been a surge in the design and implementation of distributed measurement and control systems for industrial applications. Typically, these systems are based on the client/server architecture while securing communication using the TCP/IP protocol [4–6]. Modern PLCs come with embedded web servers that provide open access to useful real time information and diagnostics that can be viewed via any standard web browser. This remote accessibility provides several advantages over more traditional solutions. For example, a problem can easily be diagnosed and perhaps fixed remotely; also engineers can have remote access to the PLC's CPU configuration tools and hence allowing for remote upload/download and configurability via the intranet or internet.

1.2. Encoding - Decoding Techniques

Modern mobile phones are able to send and receive SMS with appropriate AT commands originated from the microcontroller. The microcontroller circuit is used to control and interface between hardware devices and the SMS is generated, received, decoded and displayed through it. The complete system for SMS Gateway can be used as a base for many applications.

The SMS message can be up to 160 characters long, where each character is 7 bits according to the 7-bit default alphabet. There are two ways to send and receive SMS messages: Text mode and PDU (protocol description unit) mode. As text mode is unavailable on some phones, the PDU mode is used in this work. The PDU string contains not only the message, but also a lot of meta-information about the sender, SMS service centre, the time stamp etc. It is all in the form of hex-decimal octets or decimal semi-octets [7, 8].

Global System for Mobile Communication (GSM) has become in recent years a very common system of communication. With the great variety of GSM devices in the world market, some standardized methods of controlling the phone behavior and operations are required. Thus, the AT commands have been standardized by the European Telecommunications Standards Institute (ETSI), enabling the control of a GSM device using a microcontroller [9, 10].

1.3. Wireless Industrial Communications

Interesting approaches/standards in the context of Industrial Wireless communications may be grouped as follows:

- Proprietary protocols for radio technologies.
- Lower layer standards (IEEE 802.11 and 802.15) based on WLAN, and Sensor/Actuator Networks.
- Higher layer standards (specific Application Layer on top of IEEE 802.11 and 802.15.1 and 4, e.g. Wireless Fidelity, Bluetooth, ZigBee).
- Complete standards of mobile communications (GSM, GPRS, UMTS) and
- Ultra Wideband technology UWB, e.g. based on IEEE 802.15.3a.

The WLAN technology is being more and more introduced in the higher architecture levels of the automation hierarchy, as well as the shop floor. Bluetooth , originally developed for small range communication in the consumer market (home, PC/Notebooks, mobile phones, PDAs), is becoming increasingly interesting for the automation domain. Bluetooth consists of:

- Standard IEEE 802.15.1 (lower layers).
- Higher layer Specifications of Bluetooth.
- Profiles of Bluetooth.

Bluetooth uses asynchronous data connections with asymmetric transmission between 1 Master and 256 Slaves (up to 7 Slaves can be active Slaves). The range depends on the sender performance (max. 10m for normal applications, max. 100m for special applications). Currently, the Scatter net is in discussion. Within Scatter net, devices can be active in different Pico nets. There are successful Bluetooth applications in automation (e.g. Weczerek, 2005; Lu¨ hrs, 2005).

ZigBee (ZigBee Alliance) should be introduced to connect the automation devices at the field level, especially in the process automation with their specific Remote Terminal (RTs)requirements, because it will operate on a lower baud rate, but fortunately with low-power consumption. ZigBee consists of:

- Standard IEEE 802.15.4 (lower layers).
- Specifications by ZigBee Alliance (higher layers).
- Profiles by ZigBee Alliance.

The main features of ZigBee are:

- Low-power wireless communications.
- Less complex protocol stack.
- Very fast ‘‘Awake Phase’’ changing from power saving sleep modus to the operation modus.
- Meshed network topology is possible.
- Redundant transmission paths are possible.

Targeted application areas of ZigBee are the consumer market, building automation, and industrial automation (the focus from the beginning). Thus, the specification will be in principle suitable for sensor networks. But up to now, no profiles for applications in industrial automation are specified. The specification has been available since the end of 2004, but not all necessary functions were specified. .

Ultra Wideband Systems (UWB) are becoming more and more important for sensors and indoor location-based services. But at the moment their use is limited, because they are using the same frequency band as GSM based cell phones. The standardization activities lead to the standard IEEE 802.15.3a. Interested Alliances are WiMedia Alliance and Multiband OFDM Alliance (MBOA SIG). These alliances are targeting both the specification of UWB approaches and related certification programs. Targeted product areas are consumer electronics, mobile devices, and PCs[11].

II. Mobile SCADA Systems

Supervisory Control and Data Acquisition systems are computers, controllers, instruments; actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection .They are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms [12].

2.1 Components of the SCADA System

SCADA systems typically are made of four components:

Master Unit - This is the heart of the system, and is centrally located under the operator's control.

Remote Unit - This unit is installed from where the process is actually monitored. It gathers required data about the process and sends it to the master unit.

Communication Mode - This unit transmits signals/data between the master unit and the remote unit. Communication mode can be a cable, wireless media, satellite etc.

Software - The software is an interface between the operator and the units. It allows the operator to visualize and control the functions of the process.

2.2 Network Deployment in the Industrial Plant

On the other hand, production usually imposes quite different constraints, which result in highly specialized networks. These environments are typically high-structured and location of elements does not frequently change. Industrial networks for production (see figure 2) are arranged into hierarchical levels (plant, area, cell and field level), depending on the complexity of the overall production process. Plant level is on top, where information from lower levels is collected and the entire automation system is commanded by means of a Supervisory Control And Data Acquisition system (SCADA) [13,14]. A plant is divided into areas, which are made up of cell groups. Field level is the lowest one and includes the instrumentation: sensors and actuators.

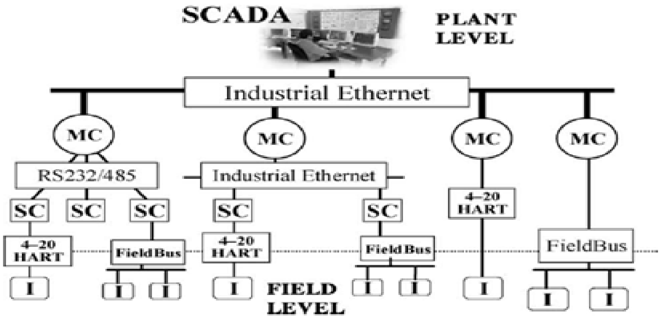

Figure 2. Network deployment in an industrial plant

In short, we have highly distributed architectures in which hierarchical control modules, mainly Programmable Logic Controllers (PLC), are interconnected by communication networks to provide both low-level control functionality and data acquisition from the instrumentation (I). Therefore, reliability and performance of the automation system greatly depend on its underlying telecommunication network.

III. The Proposed Prototype Model For PLC Based GSM Remote Control

3.1 Overview

Nowadays a lot of PLC brand names are available in the market . The most common brands are, Allen Bradely, GE Fanuc, Mitsubishi, Siemens, Toshiba and many others. As Siemens has a great market share in the industrial field, so siemens modules are suggested to be used in the proposed prototype model. Siemens has a different PLCs families starting from small plc called logo, Microcontroller Simatic S7 200, and the new version of S7 200 called Simatic S7 1200 to Simatic S7 300 and Simatic S7 400 based on the complexity of required control and automation tasks intended in the designed application [1]. In the proposed model, a Siemens Simatic S7 1200 PLC will be used because of the following:

- The micro PLC that offers maximum automation at minimum cost.
- Extremely simple installation, programming and operation.
- Large-scale integration, space-saving, powerful.
- Can be used both for simple and complex automation tasks.
- Suitable for applications where programmable controllers would not have been economically viable in the past.
- With powerful communication options (PPI, PROFIBUS DP, AS-Interface).
- Digital inputs/outputs to supplement the onboard I/Os of the CPUs.
- Function modules for simple positioning tasks (1 axis).

3.2 Hardware Structure for Siemens PLC.

Any Siemens PLC whatever of a modular type or compact type is composed of a different combinations of the following modules as shown in figure 3.

CPU	IM	DI	DO	AI	AO	FM	CP

Figure 3. Hardware Structure for Siemens PLC

1- Signal Modules

Digital input modules	DI
Digital output module	DO
Analog input modules	AI
Analog output modules	AO

2- Interface Modules
The IM360/IM361 and IM365
make multi-tier configurations possible.

3- Function Module (FM)
- Counting
- Positioning
- Closed-loop control.

4- Communication Processors (CP)
- Point-to-Point connections
- PROFIBUS
- Industrial Ethernet.
- MPI [Multi Point Interface]

3.3 Programming Languages

A variety of programming languages are used for PLC programming ,such as Ladder Diagram (LAD), Statement List (STL),Function Block (FBD), S7-GRAPH,Structured Control Language (SCL), Continuous Function Chart (CFC), and Sequential Flow Chart (SFC)[2].

A very commonly used method of programming PLCs is based on the use of ladder diagrams. Writing a program is then equivalent to drawing a switching circuit. The ladder diagram consists of two vertical lines representing the power rails. Circuits are connected as horizontal lines, i.e. in drawing a ladder diagram, certain conventions are adapted:

1. The vertical lines of the diagram represent the power rails between which circuits are connected.
2. Each rung on the ladder defines one operation in the control process.
3. A ladder diagram is read from left to right and from top to bottom. Figure 4 shows the scanning motion employed by the PLC. The top rung is read from left to right. Then the second rung down is read from left to right and so on. When the PLC is in its run mode, it goes through the entire ladder program to the end, the end rung of the program being clearly denoted, and then promptly resumes at the start .This procedure of going through all the rungs of the program is called a cycle.
4. Each rung must start with an input or inputs and must end with at least one output. The term input is used for a control action, such as closing the contacts of a switch, used as an input to the PLC. The term output is used for a device connected to the output of a PLC, e.g. a motor.
5. Electrical devices are shown in their normal condition. Thus a switch which is normally open until some object closes it, is shown as open on the ladder diagram. A switch that is normally closed is shown as closed.
6. A particular device can appear in more than one rung of a ladder. For example, we might have a relay which switches on one or more devices. The same letters and/or numbers are used to label the device in each situation.
7. The inputs and outputs are all identified by their addresses, the notation used depending on the PLC manufacture. This is the address of the input or output in the memory of the PLC. For example as shown in Figure 5, Siemens precedes input numbers by I and outputs by Q, e.g. I0.1 and Q2.0.

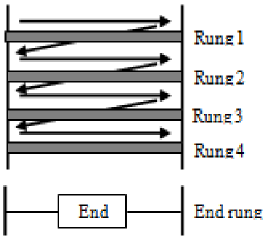

Figure 4. Scanning the Ladder Program

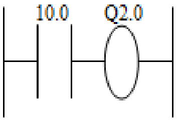

Figure 5. Siemens Rung with Input & Output

3.4 Siemens S7 Family Programming Blocks.

Siemens S7 families have a programming software package called Simatic step 7. This software is used for configuring and programming of all Simatic S7 PLCs. Also the programming of the PLC based on the following function blocks as shown in figure 6.

OB	= Organization Block
FB	= Function Block
FC	= Function
SFB	= System Function Block
SFC	= System Function
DB	= Data Block

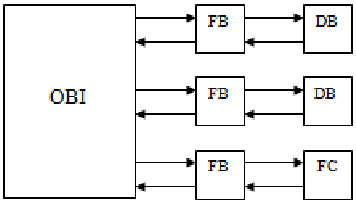

Figure 6. Siemens Programming Blocks.

Organization Block (OB)

Organization blocks is the interface between the operating system and the user program. The entire program can be stored in OB1 that is cyclically called by the operating system or the program can be divided and stored in several blocks.

Function (FC)

A function contains a partial functionality of the program. It is possible to program functions so that they can be assigned parameters.

Function Block (FB)

Function blocks offer the same possibilities as functions. In addition, function blocks have their own memory area in the form of instance data blocks.

Data Blocks (DB)

Data blocks (DB) are data areas of the user program in which user data are managed in a structured manner.

3.5 Architectural Design For The Proposed Prototype Model

3.5.1 Required Hardware and Software Components

Item Part Number	Item Specifications
6EP1332-1SH71	SIMATIC S7-1200, POWER MODULE PM1207, STABILIZED POWER SUPPLY, INPUT: 120/230 V AC, OUTPUT: 24 V DC/2.5 A
6ES7211-1AD30-0XB0	SIMATIC S7-1200, CPU 1211C, COMPACT CPU, DC/DC/DC, 6 DI 24V DC; 4 DO 24 V DC; 2 AI 0 - 10V DC, POWER SUPPLY: DC, 20.4 - 28.8 V DC, PROGRAM/DATA MEMORY: 25 KB
6GK7242-7KX30-0XE0	COMMUNICATION PROCESSOR CP 1242-7FOR CONNECTION OF SIMATIC S7-1200 TO GSM/GPRS NET
6NH9860-1AA00	SINAUT ANT 794-4MR ANTENNA GSM QUADBAND ANTENNA FOR MD720-3 UND MD740-1; OMNIDIRECTIONAL; WEATHER RESISTANT FOR INSIDE UND OUTSIDE; 5M CONNECTION CABLE"LOW LOSS" FAST CONNECTED WITH THE ANTENNA; SMA CONNECTOR; INCL. MOUNTING BRACKET; SCREWS; DOWEL;
6NH9910-0AA20-0AA0	TELECONTROL SERVER BASIC8;SINGLE LICENSE FOR 1 INSTAL-LATION;OPC SERVER FOR GPRS COMMUNICATIONWITH S7-1200 AND S7200;CONNECTION

	MANAGEMENT TO 8 REMOTE GPRS STATIONS;ROUTING BETWEEN S7 STATIONS;MULTI PROJECT-CAPABLE;WIRING DIAGNOSTICS;STATIONMONITORING TELESERVICE GATEWAY FOR STEP7;IMPORT OF SINAUT MICRO SC PROJECTS;GERMAN AND ENGLISH USER INTERFACE;DOCUMENTATION ON CD IN GERMAN AND ENGLISH.
6ES7822-0AA01-0YA0	SIMATIC STEP 7 BASIC V11 ENGINEERING-SW,SINGLE LICENSE SW AND DOCU ON DVD, CLASS A, 6 LANGUAGES(GE,EN,IT,FR,SP,CN), EXECUTABLE UNDER WINDOWS XP (32 BIT)/ WINDOWS 7 (32 BIT), FOR CONFIGURATION OF SIMATIC S7-1200, SIMATIC BASIC PANELS

Table 1. Required Hardware and Software Items

3.5.2 System Architecture

The proposed system architecture is illustrated in figure 7. The system consists of the following components:

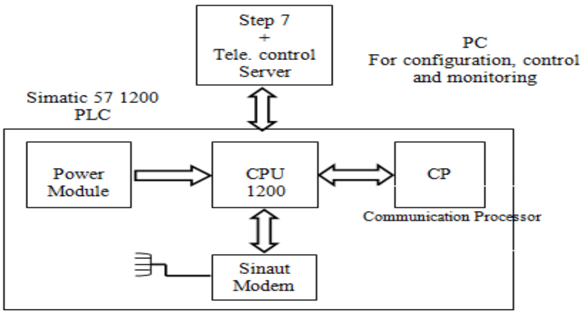

Figure 7. System Architecture for the Prototype Model.

- * A GSM SINAUT MD720-3 modem shall be coupled with a SIMATIC S7-1200 controller using a RS232 communication module and connection cable, a SINAUT ST7 connecting cable is used.
- * The SINAUT MD720-3 has a SIM card inserted and a quad-band antenna ANT 794-4MR will be used to receive the signal.
- * PLC will be wired to all controlled devices whether at home automation [heaters, air conditioning,…..etc] or at Industrial automation [Tanks, valves, motors, flow meter,…etc]. The PLC is connected to the process sensors and actuators using I/O modules.
- * CP is an integrated communication interface (hardware and software) that allows the PLC to communicate to GSM/ GPRS networks.
- * The System software was implemented mainly using Simatic Manager. The Simatic Manager environment is used for communication with the PLC system. The proposed architecture allows for programming, reprogramming, and configuring the system remotely.
- * Telecontrol server Basic 8 software will be used to manage all GSM/ GPRS communications with the PLC
- * The power supply of all components is provided via a SIMATIC PM1207 power Module.
- * As an option, the status of all controlled devices could also be monitored and controlled through the SCADA system software that is embedded in the STEP 7 software or we can use an external SCADA software.

3.5.3 System Software Architecture

The systems' software used in this prototype model is divided into three components:

- Simatic Step 7 for configuration, programming and monitoring the PLC and the process
- Telecontrol Server basic to configure the modem
- External SCADA Software for Monitoring and control [Optional]

3.6 System Configuration

3.6.1 Installing and Wiring Hardware

1. Mount all required components on a top-hat rail. Component list Table 1.
2. Wire and connect all necessary components for the remote station as described. Please watch the ground connections of the components and only activate the power supply for the SIMATIC PM 1207 at the very end.

3.6.2 Configuring Remote Station

1. Network the S7-1200 controller with your programming device. Assign the Ethernet parameter and assign an S7-1200 IP address:
2. Configure the “com [FB154]” instance data block which is called in “Main [OB1]”.

3. Select the program folder of the S7-1200 and transfer the program into the controller “Online/Download to device”. Make sure that the LED of the S7-1200 controller shows the “RUN” state.
4. Open the “PG/PC Interface” via Start/Control Panel/PC/PC Interface. Select the S7ONLINE connection as the used Ethernet network card. Confirm with OK.

3.6.3 Library and Program Blocks

With the help of the library blocks provided in table 2, wireless data transmission based on SMS is possible from the S7-1200 to other devices.

Library	Group	Program Block	Number
sms	sms_com	Function block: com	[FB 154]
		Instance data block: own name	[DB own number]
	sms_chart	chart_cmd-return	-
		chart_rs232blocks	-

Table 2. Library and Program Blocks

To be able to use the functionalities of the MD720-3 the “com” function block has to be called cyclically. When calling the “com” function block an instance data block is generated. It is recommended to assign the name “com_DB” to be able to use the description tables described below.

1- The “chart_cmd-return” watch table allows direct access to input and output parameters of the “com” function block.
2- With the help of the chart_rs232 blocks watch table point-to-point communication blocks which need the RS232 communication module can be observed.

Figure 8 shows the details of function block FB154

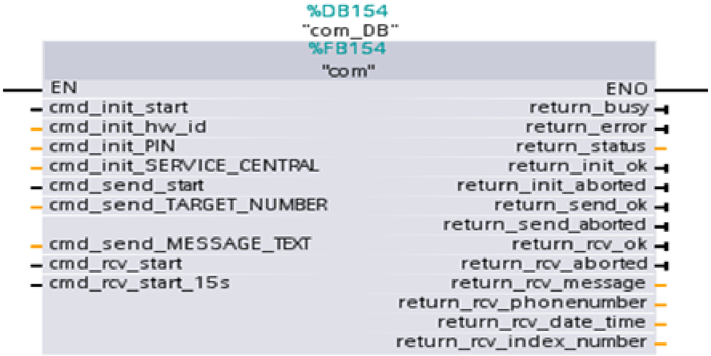

Figure 8. Function Block 154.

3.6.4 Interface Description of the Library

Figure 8 shows all parameters required for initialization, sending, and receiving processes .The parameters will be declared in the following sections:

3.6.4.1 Parameters For Initialization

No	Designating	Transmission	Data Type	Description/note
1	cmd_init_start	IN	Bool	* Enables the initialization process * Reacts to a positive edge * The start command is stored as long as the “com” function block is already in process. The block always saves only one start command provided it cannot be processed instantly
2	cmd_init_hw_id	IN	PORT	* Hardware ID of the RS232 communication module * Default value: 11; input not necessary, provided the RS232 CM was inserted in the first slot on the left of the S7-1200 and no expansion modules were inserted on the right * Check hardware ID in device information /RS232_1-Properties/RS232 interface/IO addresses/HW identifier
3	cmd_init_PIN	IN	String	* PIN number of the SIM card inserted in the modem * If the PIN number is disabled, “0000” has to be entered * Permissible value: Maximum 4 characters
4	cmd_init_SERVICE_CENTRAL	IN	String	* The short message center of your provider is to be entered here (Example: +49123456789)

				* Permissible value: Maximum 20 characters
5	return_init_ok	OUT	Bool	* Gives feedback when initialization of the modem was successful and the modem is therefore ready to operate * Stays TRUE until initialization is triggered again * Default value: FALSE
6	return_init_aborted	OUT	Bool	* Gives feedback when initialization of modem terminated incorrectly * Relevant in combination with Table 3-4 no.3 * Stays TRUE until initialization is triggered again * Default value: TRUE

Table 3. Parameters for Initialization

3.6.4.2 Parameters for SMS Sending_send_

No	Designating	Transmission	Data Type	Description/note
1	cmd_send_start	IN	Bool	* Starts the procedure for sending SMS * Reacts to a positive edge * The start command is stored as long as the "com" function block is already in process. The block always saves only one start command provided it cannot be processed instantly
2	cmd_send_TARGET_NUMBER	IN	String	* Receiver's telephone number of the device to which the SMS is to be sent * Example: +49123456789 * Permissible value: Maximum 20 characters
3	cmd_send_MESSAGE_TEXT	IN	String	* Text content of the SMS which is to be sent * Permissible value: Maximum 160 characters * Process values can be embedded with the "VAL_STRING" command
4	return_send_ok	OUT	Bool	* Gives feedback when the last job for sending SMS was terminated successfully * Stays TRUE until next job is triggered again * Default value: FALSE
5	return_send_aborted	OUT	Bool	* Gives feedback when the last job for sending SMS was not successfully terminated * Relevant in combination with Table 3-4 no. 3 * Stays TRUE until next job is triggered again * Default value: TRUE

Table 4. Parameters for Sending SMS

3.6.4.3 Parameters for SMS Receiving_rcv_

No	Designating	Transmission	Data Type	Description/note
1	cmd_rcv_start	IN	Bool	* Starts the process for receiving (retrieving) of a SMS from the modem * Reacts to a positive edge * The start command is stored as long as the "com" function block is already in process. The block always saves only one start command provided it cannot be processed instantly
2	cmd_rcv_start_interval	IN	Time	* Indicates an interval in which the process for receiving (retrieving) a SMS from the modem is started automatically * Input in milliseconds * Permissible value: >= 5000 (ms) * Interval can be ended by setting the value to <5000 (ms)
3	return_rcv_ok	OUT	Bool	* Gives feedback when the last job for retrieving SMS was successfully terminated * Stays TRUE until next job is triggered again * Default value: FALSE
4	return_rcv_aborted	OUT	Bool	* Gives feedback when the last job for retrieving SMS was not successfully terminated * Relevant in combination with Table 3-4 no. 3 * In combination with the 7030 status it is signaled that no SMS was present in the memory of the modem * Stays TRUE until next job is triggered again * Default value: TRUE
5	return_rcv_me ssage	OUT	String	* Displays the SMS text content
6	Return.rcv.pho.nenumber	OUT	String	* Indicates the number of the device from which the SMS was sent
7	return_rcv_date_time	OUT	DTL	* Indicates the time stamp which is saved in the SMS * This is the time stamp which the provider provides at the time of delivery. This is not the time stamp at the time of sending the SMS from the cellular phone or remote station. * The elements "Nanosecond" and "Weekday" of the DTL time format are not present
8	return_rcv_index_number	OUT	Int	* Indicates the index number of the SMS from the modem memory of the modem

Table 5. Parameters for Receiving SMS

3.6.4.4 Return Parameter: return_

No	Designating	Transmission	Data Type	Description/note
1	return_busy	OUT	Bool	* Signals when the "com[FB154]" block is busy with processing a routing * Takes on the TRUE state once a "cmd_" command was triggered. * Can also take on the TRUE state when the RCV routine is called cyclically with the help of the "cmd_rcv_start_interval" parameter. * Takes on the FALSE state as soon the routine is terminated
2	return_error	OUT	Bool	* Gives feedback if an error occurred during the processing of a routine * Always relevant in combination with Table 3-4 no. 3
3	return_status	OUT	Int	* In the case of an error, returns the status to be able to localize the cause of the error * Always to be noted in combination with the status list from Table 4-1

Table 6. Return Parameter

3.7 System Operations

3.7.1 Configuration of the SIMATIC Controller and Modem Registration on the GSM Network

The steps for configuring the Sematic Controller and the Modem are described as following:

1- During initialization the RS232 communication module is configured for ASCII based communication with the SINAUT modem. After the configuration**,** the RS232 communication module is set as follows:
   * Communication protocol: Point-to-Point communication protocol
   * Transmission speed: 19.2 Kbit/s
   * 8 data bits per character
   * Parity: No parity
   * Stop bit: One stop bit

2- The **short message center** of the provider is stored in the modem. This is done once during initialization and all following routines for sending SMS automatically use this center in the provider infrastructure for SMS messaging.

3- The modem automatically logs onto the provider's GSM network, provided the **PIN** number of the inserted SIM card was validated.

3.7.2 The Initialization Routine in Details

During this initialization phase, each step is monitored. If a step cannot be performed, this leads to a respective comment in the status word. The initialization routine is cancelled.

If the above step chain terminates neither positive nor negative after a maximum of 60 seconds, the routine is canceled.

3.7.3 Sending Text Messages

With the help of the "com [FB154]" function data block, text messages can be send provided the appropriate parameters are set. Figure 9 shows the flow chart for sending routine.

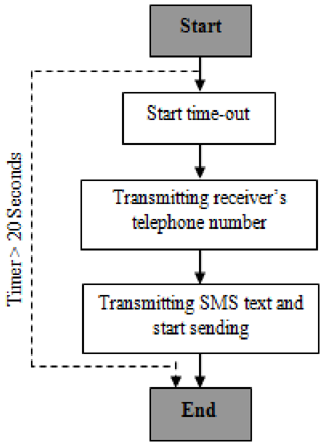
Start
Start time-out
Transmitting receiver's telephone number
Transmitting SMS text and start sending
End
Timer > 20 Seconds

Figure 9. Flow Chart for Sending Routine.

During this routine for sending SMS, every step is monitored. If a step cannot be performed, this leads to a respective comment in the status word. The routine is interrupted.

If the above step chain terminates neither positive nor negative after a maximum of 20 seconds, the routine is canceled.

3.7.4 Receiving Text Messages

Figure 10 shows flow chart for receiving routine .

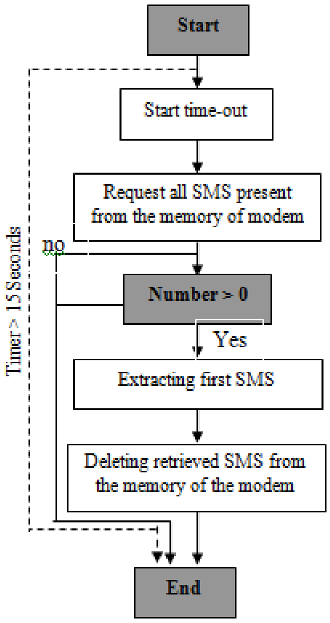
Start
Start time-out
Request all SMS present from the memory of modem
no
Timer > 15 Seconds
Number > 0
Yes
Extracting first SMS
Deleting retrieved SMS from the memory of the modem
End

Figure 10. Flow Chart for Receiving Routine.

From figure 10, during this routine for receiving SMS, every step is monitored. If a step cannot be performed, this leads to a respective comment in the status word. The routine is interrupted.

If the above step chain is terminated neither positive nor negative after a maximum of 15 seconds, the routine is interrupted.

Always only one SMS is retrieved and this SMS is immediately deleted from the modem's memory after transmission to the S7-1200 controller. therefore It has to be sure that the content of the previous SMS was successfully processed between two receive routines.

It cannot be ensured that the SMS is stored in the modem's memory in the correct time sequence and is retrieved from there accordingly**.**

3.8 Economical Study

Table 7 shows that the total cost of the prototype components should be $ 1,678.90USD . The cost may be exposed to a slight differences in the total cost based on the applied taxes and customs in every country.

Item	**Order No.**	**Qty**	**List**
Basic Hardware Components			**Price/Unit $**
10	6EP1332-1SH71	1	87
20	6ES7211-1AD30-0XB0	1	188
30	6GK7242-7KX30-0XE0	1	522
40	6NH9860-1AA00	1	45.90
50	6NH9910-0AA20-0AA0	1	470
60	6ES7822-0AA01-0YA0	1	366
	Grand Total		**1,678.90**

Table 7. Total Coast of Prototype Model

IV. Conclusion

In this paper the concept of GSM based remote control system has been discussed. A brief description on the Microcontrollers, Programmable Logic controllers and SCADA systems has been mentioned. The Coding and decoding techniques in GSM based control are explained. In Addition to that the wireless communications in the industrial field are detailed. A newly proposed prototype system for integrating Home/Industrial GSM based remote control has been fully and economically discussed. The Future work will be devoted on how the prototype model will be converted to a pilot project.

Reference

[1]. B. Ramamurthy, S. Bhargavi and R. Shashikumar, "Design and Implementation of GSM based Remote Monitoring and Control system for Industrial process Parameters", International Journal of Computer Science and Internet Security (IJCSIS) , vol. 8, No. 5, PP. 219–225. 2010.

[2]. S. D. Sharma and R. S. Kasana, "Research Issues and Challenges of Mobile Database Systems", International Journal of Computer Information Systems (IJCIS), vol. 2, No. 2, PP. 28-31, 2011.

[3]. C. K. Das, M. Sanaaullah, H. M. G. Sarwer and M. M. Hassan, "Development of a Cell Phone Based Remote Control System: on Effective Switching System for Controlling Home and Office Appliances", International Journal of Electrical & Computer sciences IJECS, Vol. 9, 2010.

[4]. Sungmo Jung, Jae-gu Song, Seoksoo Kim, "Design on SCADA Test-bed and Security Device," International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 4, October, 2008.

[5]. Surve, V, 2006, "A wireless Communication Device for Short Messages", Masters Thesis, Available: www.certec.lth.se/doc/awireless.pdf.

[6]. Kim, Eung Soo, Kim, Min Sung, "Design and Fabrication of Security and Home Automation System", ICCSA, International Conference Computational Science and Its Applications, Proceedings, Part III, P. 3137, 2006.

[7]. GSM SMS and the PDU format, http://www.dreamfabric.com/sms accessed on 5 March, 2008

[8]. Michael Harrington, "Understanding SMS: Practitioners Basics" http://mobileforensics.files.wordpress.com/2007/06/understanding_sms.pdf accessed on 24 February, 2008

[9]. W.C.Y. Lee, "Spectrum Efficiency in Cellular," IEEE Trans. on Veh. Tech., vol. 38, no. 2, May 1989.

[10]. W.C.Y. Lee, "Spectrum Efficiency and Digital Cellular", 38th IEEE Veh. Tech. Conf. Records, PP. 643, June 1988.

[11]. Peter Neumann, "Communication in Industrial Automation", Science Direct, Control Engineering paradise 15, PP. 1332-1347, 2007.

[12]. Hildick-Smith, Andrew, "Security for Critical Infrastructure SCADA Systems," (SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, February 2005),

[13]. CERN Website, SCADA Explanation, in: http://ref.cern.ch /CERN /CNL/2000/003/scada/.

[14]. The HART communication protocol specification, in: http://www.hartcomm.org/technical/doclist.html.