

# Development of a Gateway to PROFIBUS for Remote Diagnostics

Hassan Kaghazchi, Donal Heffernan  
Automation Research Centre, University of Limerick, Ireland

## Abstract

With the increased use of fieldbuses in distributed control systems, the management and maintenance of these networks becomes an issue, especially where only a limited knowledge base is available at the plant level. Continuous monitoring of fieldbus networks offers the advantage of identifying some of the potential problems before they lead to loss of communications and plant shut down. Remote monitoring capability offers the advantage of providing access to a wider pool of experts to diagnose network problems. This research will demonstrate the concept of a passive gateway as a proxy between PROFIBUS and Ethernet networks. The gateway can record diagnostics, configuration and error telegrams, and will use a fuzzy logic approach in determining the potential problems.

## Introduction

The lack of a unified approach to PROFIBUS diagnostics presents a substantial problem, mainly to the end user. As the number of vendors increases in a plant, the problem of diagnosing the multitude of devices from different suppliers escalates. Although the international fieldbus standards such as IEC 61158[1] sets out the details of how each device can communicate the diagnostics data, the extent to which this diagnostics data is used and converted to meaningful information by the vendor's configuration/programming tool varies considerably from one supplier to another.

The problem can be compounded in the case of multi-master systems where the diagnostics data is kept in different formats by individual masters, and would require additional programming effort to extract the required diagnostics data.

The suppliers' approach to the solution of this problem has been generally limited to the diagnostics capability of their respective configuration/programming packages, while some vendors have gone a bit further and provide specific diagnostics function blocks and sample SCADA screens for visualisation of basic diagnostics information for a particular CPU [2].

Third party companies have recognised the problem and have addressed it by producing PC based software packages, which can connect to the PROFIBUS network using a PC interface card.

These packages can provide the user the access to raw diagnostics telegrams on the bus irrespective of the make of the equipment. Some of these packages can provide the mandatory diagnostics data in a more comprehensive textual format [3].

Again this is manual method and requires a high level of familiarity with the details of the

PROFIBUS protocol. As the number of devices increases on the network this method of analysis become impractical. Additionally, for the devices that can provide extended diagnostics this method would require cross-reference with the device GSD file to decode the data.

The objective of the research work presented here is to define a functional specification for a gateway for the online monitoring of all devices on a PROFIBUS network. It is intended that the diagnostic information, mainly in graphical format, will be available both within a plant as well as remotely from outside the plant.

## Diagnostics Mechanism in PROFIBUS-DP

PROFIBUS is a master-slave network, based on a token passing medium control access scheme between master stations. When a master has the token it communicates with its associated slaves and then passes on the token to the next master station in a logical ring (Fig1).



Fig 1: Master-Slave Communications in PROFIBUS

The communication between master and slave is accomplished using a set of telegrams: Configuration, Parameterisation, Data Exchange, and Diagnostics [4]. While in normal data exchange mode, if a slave has diagnostics data it flags this by returning "0A" in the "Function Code" of returned data exchanged telegram. (Fig2).

master and its associated slaves and a programming package is required for writing instructions to pass data between devices. In some cases these two packages are combined into one [3].

SD	LE	LEr	SD	DA	SA	FC	DSAP	SSAP	DU..	FCS	ED
68H	x	x	x	8x	8x	x	62/3E	60/3C	x ..	x	

SD: Start Delimiter  
 LE: User Data Length + DA, SA, FC, DSAP, SSAP  
 DA: Destination Address  
 SA: Source Address  
 FC: Function Code (FC=0A Signals Diagnostic Data)  
 DU: Data Unit  
 DSAP: Destination Service Access Point  
 SSAP: Source Service Access Point  
 FCS: Frame Checking Sequence  
 ED: End Delimiter

Figure 2: Request/Response Frame PROFIBUS-DP

In the next telegram from the master a diagnostic request is sent to the slave, and the slave replies with diagnostics data (Fig3). Each slave has to send six bytes of mandatory diagnostics data.

DP	14	NIL	6	NIL	Response	Data Exchange	10 20 30 40
DP	6	NIL	7	NIL	Request	Data Exchange	00 00
DP	7	NIL	6	NIL	Response	Data Exchange	00 00
DP	6	NIL	14	NIL	Request	Data Exchange	00 00 00 00
DP	14	NIL	6	NIL	Response	Data Exchange	10 20 30 40
DP	6	NIL	7	NIL	Request	Data Exchange	00 00
FDL	7	NIL	6	NIL	Response	DH	00 00
DP	6	62	7	60	Request	Slave Diagnose	
DP	7	60	6	62	Response	Slave Diagnose	08 0C 00 06 80 2F 42 02 14 01 02 01 01 0B 04
DP	6	NIL	14	NIL	Request	Data Exchange	00 00 00 00
DP	14	NIL	6	NIL	Response	Data Exchange	10 20 30 40
DP	6	NIL	7	NIL	Request	Data Exchange	00 00
DP	7	NIL	6	NIL	Response	Data Exchange	00 00



Figure3: Slave sends a Data High in FC code to flag existence of Diagnostics Data

Additionally if the slave is capable of providing extended diagnostics it can send up to 240 bytes of extended diagnostics to the master. The extended diagnostics data is subdivided into: Device (station) related, Identifier (module) related and Channel related diagnostics. By using a suitable tool to analyse the diagnostics data some valuable information about the health of the individual device can be obtained. The following section is a brief overview of some existing methods for PROFIBUS network diagnostics.

### Diagnostics Tools

#### Programming tools

There are two sets of software tools required for setting up and operating a PROFIBUS-DP network. A configuration package is required to set-up a

No.	TL	Function	Event
13	...	DP-Slave	Slave is ready for data transfer.
12	...	DP-Slave	Master (PROFIBUS addr 1) releases the slave for other masters.
11	...	DP-Slave	Slave is ready for data transfer.
10	...	DP-Slave	Configuration adopted.
9	!	DP-Slave	Timeout occurred.
8	...	DP-Slave	Slave is ready for data transfer.
7	...	DP-Slave	Parameters reassigned by other master (PROFIBUS addr:25) with status byte 0x88.
6	...	DP-Slave	Slave is ready for data transfer.
5	...	DP-Slave	Configuration adopted.
4	...	Mgt	I/O enable by S7 CPU
3	...	Mgt	I/O disable by S7 CPU
2	!	P-Bus	Protocol error in miniprotoکل.
1	!	P-Bus	Frame error on I/O bus.

Figure 4: Diagnostics Information for CP342-5

Typically, such packages provide some level of diagnostic features, depending on the make and model of the devices used on the network. Each manufacturer presents their diagnostics information in different formats and a good familiarity on users' side is required to access and interpret the diagnostics data. Figure 4 shows a typical display from one of these packages

Apart from diagnostic features, in general one configuration package and one programming package are used with each type of master. As the number of masters of different makes increases the number of required packages increases, giving rise to unnecessary complexity.

#### Diagnostic Function Blocks

As stated earlier, some manufacturers have developed special function blocks, which are capable of diagnosing individual slave devices. These function blocks when called can instruct the master to send a diagnostics telegram to a particular slave and store the returned diagnostics information in a data block. This data block on the master can be accessed by, for example, a Supervisory Control And Data Acquisition (SCADA) system and the diagnostic information can then be displayed on a PC screen. In addition to mandatory single slave diagnostics data and extended slave diagnostics, other information can be stored in this data block, such as:

- ≡≡ List of configured slaves
- ≡≡ List of failed slaves
- ≡≡ List of faulty slaves
- ≡≡ List of existing slaves, including slaves of other masters

Further work is required on the standardisation front to establish an exact format to which the diagnostics data blocks should adhere to. This would enable different vendors to develop function blocks for their respective masters and include these in the library of their programming tools for the benefit of the end user.

*IT-Cards*

With advances in IT technology PLC vendors have moved towards development of Ethernet based communication cards with IT functionality (eg Siemens CP343-1IT & Mitsubishi QJ71WS96). These units can act as web servers and provide some Java Beans and Applets for aiding the end user in developing a Java interface to read and write variables remotely from/to the PLC and also to support the downloading of programs. Only a web browser is required to remotely access the IT cards from anywhere.

Once the diagnostic data block format is defined, then the Java interface would read this data block and present it to the user in a more 'graphical' format. Obviously if the diagnostics data block structure stays the same for all the vendors then the Java interface would obtain data over the Internet from individual masters, irrespective of their make.

*PC-Based Analysers*

PC-based analysers consist of a software package and a PC card. These analysers provide access to all the traffic on the bus, in real time. The use of analyser requires a high level of expertise with PROFIBUS. Table 1 shows a list of some of the available analysers on the market.

<i>Analyser</i>	<i>Supplier</i>	<i>Price</i>	<i>Hardware Requirement</i>
Amprolyser V3.0	Comdec	€250	Siemens CP5611
Profiscope	Trebing & Himstedt	€1290	Siemens CP5511 CP5611
Profibus Analyser	TMG I-Tec	€980	Siemens CP5613 CP5412
Profibus Analyser	Softing	€4970	Softing Hardware
SioCheck	Autem	€533	RS 485 port

Table1: Some of the available PROFIBUS analysers

All or some of the PROFIBUS telegrams can be captured and analysed. Typically an "expert" is needed to manually analyse/interpret the data. Although this method provides a transparent access to all the telegrams on the bus, the fact that a high level of expertise is required and the time it may take to analyse the data at bit and byte level, makes this method unsuitable from a practical point of view. Additionally an analyser takes just a snap shot of the traffic on the bus (Fig5) and therefore cannot be considered as proper on-line analysis method.

<i>L2 Service</i>	<i>Sd</i>	<i>Adr</i>	<i>Sap</i>	<i>Fc</i>	<i>Len<sub>Msg</sub></i>	<i>Len<sub>Data</sub></i>
Srd_High	SD2	007 -> 013		7D	11	2
DH	SD2	007 <- 013		0A	13	4
Srd_High	SD2	007 -> 013	3E -> 3C	5D	11	0
DL	SD2	007 <- 013	3E <- 3C	08	40	29
OK	SD1	007 <- 024		00	6	
Srd_High	SD2	026 -> 016		5D	11	2
OK	SC				1	

Figure5: Display from Siemens Amprolyser

*Diagnostics Repeater*

A diagnostic repeater can provide diagnostics data from the PROFIBUS (Fig6) cable during plant operation. It acts as a slave on the network and can communicate diagnostics information to the master. This diagnostic information consists of fault types such as: wire break of the PROFIBUS cable, short circuit of one of the conductors to the shield, missing terminator resistors, two or more measurement circuits for diagnostics in one segment, loose contacts, cascading depth violation, too many nodes in the segment, nodes too far away from diagnostics repeater, and faulty PROFIBUS messages [5]. The location and type of the fault on the cable is provided in text format. The diagnostic repeater mainly deals with cabling related problems, and other network related diagnostics should be undertaken using other complementary measures.

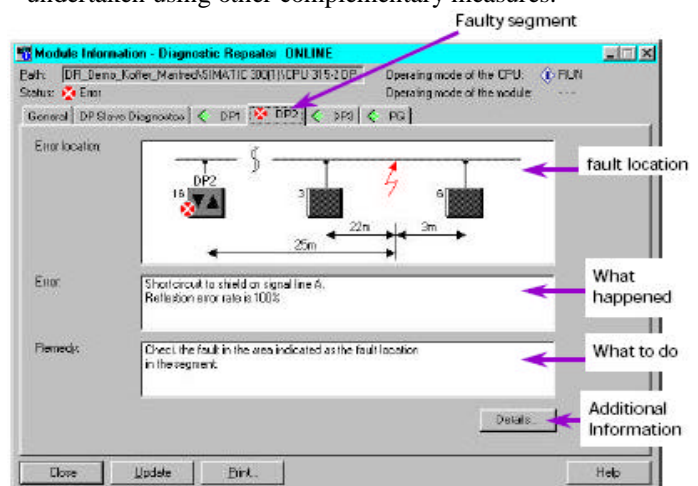


Figure 6: Information from Diagnostics Repeater

### A New Diagnostic Gateway Concept

So far we have looked at the various types of available tools for PROFIBUS network diagnostics. No single tool is capable of providing the online diagnostics functions necessary for best-practice network management and plant maintenance. The objective of our research work is to define the concept of a PROFIBUS-Ethernet gateway, which is capable of online diagnostics on the PROFIBUS networks with web server functionality. The proposed gateway will be a “plug & play” item, and will reside on PROFIBUS and Ethernet networks simultaneously. It will act as a master class 2 on PROFIBUS and will have its own IP address on Ethernet, where a TCP/IP layer will be running on top of the Ethernet.

Once installed the gateway will build a graphical representation of the actual PROFIBUS network showing all the masters and their associated slaves. The status of the devices will be identified as: operating, faulty or failed. On the screen, the user can click on the device to get further diagnostics information such as device related, module related or channel related data.

The experimental PROFIBUS-DP network (Fig7) at the Automation Research Centre is currently being used to develop the prototype gateway and demonstrate the concept. This network has over 30 PROFIBUS nodes consisting of PLC, HMI, PROFIBUS/AS Interface, Operator Panel, VSD and so on. To demonstrate the concept of the project a Siemens CP5611 (master class 2) is set-up as the “Gateway” (see Fig6) between the PROFIBUS-DP network and Ethernet. It acts as an OPC (OLE for Process Control) server to pass the diagnostics information to a Java based client with a user interface.

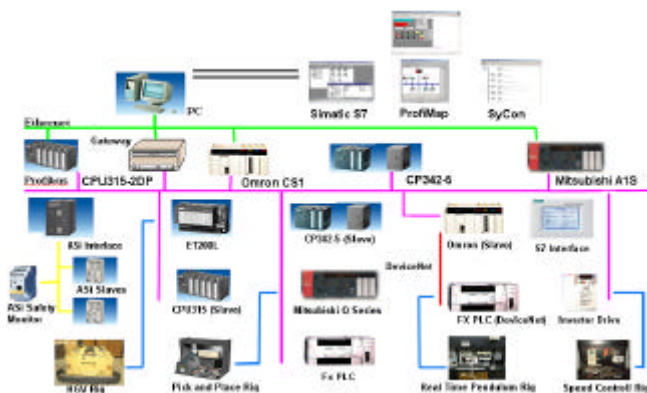


Figure 7: CP5611 as master class 2 connected to DP network

Using OPC the gateway can provide the following functions [6]:

- ≡≡ Set slave address
- ≡≡ Get slave configuration data
- ≡≡ Get slave diagnostics data
- ≡≡ Read slave inputs/outputs
- ≡≡ Get master data transfer list  
*Shows the slaves involved in data exchange*
- ≡≡ Get master diagnostics  
*Shows if any slave has signalled extended diagnostics*
- ≡≡ Get master state  
*Stop, Clear, Operate, Ident-Number, Hardware/Firmware version*

The access to the prototype gateway can be from inside or outside of the plant, and only a web browser will be required for accessing the diagnostics information. Fig8 shows the current prototype’s format for the information, which is displayed in the browser. The stations with no diagnostic are displayed in green, faulty stations in yellow, and failed stations in red. To obtain further information the user can click on a particular station and more information is displayed in the lower pane.

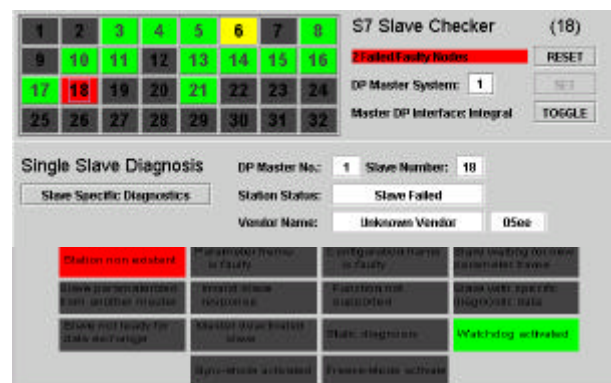


Figure 8: Prototype gateway PROFIBUS-DP diagnostics information

A big challenge in this project is to be able to retrieve diagnostic information from different types of masters and to present this data in a common interpreted format for the user. The authors, by using reverse engineering approaches, can show how to do this for some different types of masters. However, the longer-term goal of the research project is to propose a fully standardised approach that might be adopted by the fieldbus standards into the future.

## Conclusions

Different approaches for the diagnostics of PROFIBUS networks have been outlined. The information which they provide range from simple information codes to masses of data, the latter requiring an expert knowledge. None of these methods provide continuous on line diagnostic information.

A solution to this problem is addressed by developing the concept of a PROFIBUS-Ethernet gateway for online PROFIBUS network diagnostics. The gateway will operate on a “plug & play” principle, using an OPC server, representing the information in graphical format over Internet.

The current phase of the project is concerned with the functional specification of the proposed gateway, and testing of some of its intended functionality by using a PC equipped with a PROFIBUS CP. The next phase of the project will involve the complete design, build and testing of this gateway.

## Acknowledgement

The authors gratefully acknowledge the Irish State agency, Enterprise Ireland, for the support of Commercialisation Fund of Enterprise Ireland – Project number PC/2003/002

## References

1. CLC/prTR 61158-1:2004. IEC Standard Document. “Digital data communications for measurement and control – Fieldbus for use in Industrial Control systems – Part 1: Overview and guidance for IEC 61158 series. IEC, 2004.
2. PROFIBUS Diagnostics Package for Simatic S7 and WinCC, ID:6095050  
<http://www4.ad.siemens.de/WW/llisapi.dll?func=cslib.csinfo&objAction=csBrowse&lang=en&siteid=CSEUS&objId=4000590>
3. PROFIBUS Scope, for CP5611/CP5511, Trebing & Himstedt, <http://www.t-h.de>
4. Popp, M,” The New Rapid way to PROFIBUS DP”, PNO,  
<http://www.Profibus.com> order No.4.072
5. Simatic Diagnostics Repeater for PROFIBUS-DP Manual, order number 6ES7972-0AB00-8BA0, Edition 12/02
6. Simatic Net DPMCL2 Programming Interface Manual C79000-B8976-C121-04