IDX TECHNICAL SPECIFICATIONS

PROFIBUS Audit Procedure and Checklist

Revision 1.0, March 2022

Table of Contents

1. Introduction

The purpose of this document is to support the PROFIBUS network audit process. This document provides the reader with the knowledge required to examine the installation and assembly of PROFIBUS networks.

The presentation of information has been kept as simple as possible to ensure understandability. However, this document does not replace any training that is required to suitably analyse and troubleshoot PROFIBUS networks. A PROFIBUS audit should be completed by a Certified PROFIBUS Engineer.

2. Safety Information

The use of this document may involve the handling of hazardous materials or dangerous tools as well as risky work on the related site. Due to the diverse applications of PROFIBUS and the various demands that each system presents, it is not possible to consider all options or safety requirements.

For you to competently judge possible dangers, inform yourself of the safety requirements for the respective systems before starting work. This includes adhering to the laws and regulations of the respective country in which the system is operated as well as observing the health and safety requirements for the company in which the system is being audited.

3. Common Faults and Network Diagnostics

For a detailed list describing the typical faults that can occur in a PROFIBUS network and how to go about identifying and correcting these faults, refer to IDXT0102 PROFIBUS Fault Finding Procedures.

For additional information on network diagnostics, refer to *IDXT0006 Control Network Diagnostics*.

4. Audit Requirements

For an audit to be completed successfully, the following are required:

- The audit MUST be carried out by a Certified PROFIBUS engineer.
- All applicable required fields in the audit checklist must be completed.
- All required additional documentation must be attached to the report.
- The full audit checklist and report summary must be submitted to the Client.

5. Tools Required

A PROFIBUS Engineer is rendered blind to a network unless he has the correct tools available that enable him to analyse the true state of the network's health, retrieve network statistics and view the network's electrical signal on the copper cores. To effectively determine the health of a PROFIBUS network and find faults quickly, a PROFIBUS engineer should keep the following items in his tool bag:

5.1. PROCENTEC ProfiCore and ProfiTrace software

Otherwise referred to as the PROFIBUS Troubleshooting Toolkit, this essential piece of equipment allows you to connect to a currently running PROFIBUS network and analyse critical aspects of the installation.

The ProfiTrace software provides certified personnel with the information that they need to quickly identify and resolve PROFIBUS faults. It features a live-list, integrated oscilloscope for analysis of the differential signal as well as the individual A and B core signals, a bar graph that displays the driver voltages for all devices across the network, message recording functionality for in-depth analysis of the telegrams being sent over the bus, and a variety of useful network statistics such as lost devices, syncs, and illegal messages.

It also features reporting capabilities, allowing personnel to generate weekly, bi-weekly, or monthly reports and to actively monitor the network health.

Note: The oscilloscope and bar graph analysis are limited to devices on the same segment that the PROFIBUS Troubleshooting Toolkit is attached. To analyse all devices across the network the PROFIBUS Troubleshooting Toolkit will need to be attached to every segment of the network. Report generation should be limited to the relevant devices on each segment using the Network Manager functionality in ProfiTrace and dividing your network into segments, measuring points, and linking in the appropriate devices.

5.2. PROCENTEC Mercury tablet

The PROCENTEC Mercury is a multi-protocol analyser. With industrial Ethernet gaining traction, it is important to have a tool available that is capable of properly troubleshooting existing PROFIBUS networks as well as newly installed/upgraded Industrial Ethernet networks.

The Mercury is supplied with an industrialised tablet running the OSIRIS software. The OSIRIS software allows you to choose between PROFIBUS and Industrial Ethernet troubleshooting. From a PROFIBUS troubleshooting perspective, the OSIRIS software, similar to the ProfiTrace software, features a live-list, a built-in oscilloscope, a bar graph that displays the driver voltages for all devices across the network, message recording functionality, and a variety of useful network statistics such as lost devices, syncs, and illegal messages.

Note: The oscilloscope and bar graph analysis are limited to devices on the same segment that the Mercury is attached. To analyse all devices across the network the Mercury will need to be attached to every segment of the network. Report generation should be limited to the relevant devices on each segment using the Network Manager functionality in ProfiTrace and dividing your network into segments, measuring points, and linking in the appropriate devices.

The Industrial Ethernet mode provides personnel with insight into their Industrial Ethernet networks with various features including a topology view, device connection status, and device information. The compact industrialised tablet makes this tool ideal for on-site troubleshooting, eliminating the need to carry a laptop around the plant with you.

It also features reporting capabilities, allowing personnel to generate weekly, bi-weekly, or monthly reports and to actively monitor the network health.

5.3. PROCENTEC ComBricks

With PROCENTEC ComBricks you have a valuable permanent monitoring solution for your PROFIBUS networks and when combined with the NCI (network condition indicator) software, the ability to monitor the health of all PROFIBUS networks across the site from one central location.

ComBricks is a modular solution and can be expanded as required, it is a transparent device and therefore does not require any PLC configuration, simply connect it to the network and it is ready to go. It incorporates ProfiTrace OE (Over Ethernet) and from the web page of the ComBricks, you have access to a wealth of information including signal waveform analysis, bar graph driver voltage analysis, critical network statistics, and message recording functionality.

With ComBricks installed to constantly monitor your PROFIBUS networks, you have a history of events that have occurred which is extremely useful for troubleshooting those pesky intermittent network faults that always seem to occur after hours.

ComBricks can be configured to send email notifications when a fault has occurred or is likely to occur, allowing you to act immediately and mitigating unnecessary network downtime. By utilising a secure VPN connection to ComBricks, you have a permanent monitoring solution that you will have access to from anywhere in the world.

For more detail on PROFIBUS Permanent Monitoring, please see the separate documents *IDXT0007 Control Network Permanent Monitoring.*

5.4. PROFIBUS cable stripping tool

A Stanley knife is not a practical PROFIBUS cable stripping tool and often results in wiring errors being introduced in the form of A-B shorts or a shield short to one of the cores. The PROFIBUS cable stripping tool features two blades set to specific depths, one blade removes the shield exposing the A & B cores and the other blade just removes the outer sheath exposing the shield. Once set, it perfectly prepares the PROFIBUS cable each time.

5.5. AC clamp meter

It is very useful to be able to measure the current that is travelling on the PROFIBUS cable shield. The excessive current travelling on the shield is often caused by potential differences across the network and/or poor functional grounding implementation. The appropriate AC clamp meter should be capable of measuring high-frequency current up to 100kHz.

6. Audit Procedure

The process of a network audit must include the physical and visual checking of all network components for any damage and proper installation. Any discoveries made during the audit will need to be documented for the client and used within the reporting recommendations made by the engineer after the audit. A network audit can be carried out in the following steps:

6.1. Network history

It is very challenging to audit and troubleshoot a network if the network diagrams/topology layouts are unavailable. Before you arrive on-site, request these diagrams from your client. The diagrams must match the installation, and this should be checked.

The following items should be included on network diagrams or supporting documents:

- Segments (including Type DP / PA)
- Order of devices
- Addresses of devices
- Termination points
- Cable Lengths
- Repeaters, Diagnostics Repeaters, Couplers, OLMS
- Locations of devices (Area, Cabinet etc)
- Type of devices (incl. Make, Model, Ident No)
- Access points (PG plugs)

6.2. Visual inspection

A visual inspection will often reveal obvious problems and should be carried out first. The engineer must execute a physical inspection of the network components to identify any damage or installation issues that may exist and to ensure that the correct connectors are used and properly installed/wired.

This should include an inspection of the:

- Terminations (especially at repeaters and VSDs)
- Cabling (Type of cabling, cable clearance from high voltage etc)
- Connectors (Proper wiring, certified connectors, no shield exposed)
- Components (Certified devices, proper device grounding, ingress ratings)
- Power Supplies

If problems are spotted at this level, ask the client if they wish to correct these problems before you continue with the audit. Some time for correction of small errors should always be included in an audit and any repairs that are made must be listed in the corrections section of the audit report.

6.3. Network inspection, network scan and segment report generation

During the network inspection, an electrical analysis of each of the network's segments will be conducted. This will allow the engineer to identify problem devices; determine the network speed; analyse the signal waveform, driver amplitudes, and in some cases, the network topology. These data tools are critical for identifying what is causing problems within the network.

Report generation should be limited to the relevant devices on each segment using the Network Manager functionality in ProfiTrace and dividing your network into segments, measuring points, and linking in the appropriate devices. A report should be generated for each segment on the network ideally from the beginning and end of each segment.

Consider using ProfiCaptain, if licenced, to undertake a Network Scan. Ensure your Class 2 Master is set to a free address and isn't a duplicate of the Network Class 1 Master (e.g., PLC usually address 1 or 2) or any of the Slaves, and that it runs at the same baud rate as the network.

6.4. Report writing and submission

Following the network audit, the engineer is required to write a report detailing what they have discovered on the network during the fieldwork. Any faults identified and fixed should be listed along with all the faults that could not be fixed and how the site technicians can go about correcting these faults. Further recommendations regarding health and sustainability may be listed for the site personnel to implement.

6.5. Follow-up

After the report submission, the engineer may do a follow-up with a client to check if the network is still functional and check if the recommendations have been implemented or not and discuss the effect the scheduled changes may have on network availability and uptime. This will also help with checking if there may be a need to schedule an audit earlier than the annually scheduled audit.

7. Audit Checklist

Company:		
Site:	Network:	
Baud rate / Speed:	Number of segments:	
Number of PROFIBUS Masters:	Number of PROFIBUS Slaves:	
Number of transparent devices:	Includes PA:	Yes / No
Engineer:	Date:	

Visual Inspection	Yes	No
Are there two and only two terminations per segment?		
Is there any cable shielding exposed on the PROFIBUS DP connectors?		
Are all the PROFIBUS DP connectors correctly built and fastened?		
Are there specific devices (e.g., VSDs) that have built-in terminations and are they all correctly set (e.g., OFF if not the first or last device in the segment)?		
Are the cable and segment lengths below their respective baud rates?		

Baud Rate	Max Segment Length	Overall Max Cabling Length	Stub Lines
9.6 Kb/s	1,000m	10,000m	Not prescribed/any amount
19.2 Kb/s	1,000m	10,000m	500m
45.45 Kb/s	1,000m	10,000m	200m
93.75 Kb/s	1,000m	10,000m	100m
187.5 Kb/s	1,000m	10,000m	33m
500 Kb/s	400m	4,000m	20m
1.5 Mb/s	200m	2,000m	6.7m
3, 6 & 12 Mb/s	100m	1,000m	None allowed

Visual Inspection (cont.)	Yes	No
Are the correct cables being used for each segment (e.g., PROFIBUS DP vs PROFIBUS PA)?		
Is the correct cable type being used for the application/environment? *Note: Outer PVC coating suited for the environment? Single-core cable vs stranded-core?*		
Is there at least one meter of cable between all connectors?		
Has the outer cable insulation been removed?		
Has the exposed shielding been clamped to the cabinet earth bar/backplate where cables enter and leave?		
Is the shielding continuous throughout the entire segment, and grounded at multiple points?		
Is the PROFIBUS cable correctly separated from other higher voltage cables, following the cable separation guidelines?		
Is the cable bend radius for all RS-485 cabling above 75 mm for a single cable and above 150mm where it is looped in a circle?		
Are all the repeaters, OLMs, devices (e.g., Drives, Simocodes, Meters etc.) and hubs powered and operating correctly?		
Are the dip switches on the devices correctly set, and matching addressing where applicable?		
Are the total number of PROFIBUS devices on the network under 125?		
Are the number of RS-485 devices (incl. Repeaters, OLMs, Couplers) 32 or less per segment? Good practice would dictate less than 25 devices on a segment.		
Are there any devices with an off-the-shelf/reserved address of 126?		
Do the OLMs, specifically within a network, have the same firmware, software, and hardware?		
Are the OLMs in the correct data transfer mode? *Note: There are various modes such as compatibility mode, ring/redundancy mode, and standard operating modes. The correct mode*		

	Yes	No
should be used depending on requirements, and this should be the same on each OLM within the network transferring data.		

Per Network	Yes	No
Check the network statistics for slaves/devices for the following:		
• Are you able to access each segment with a ProfiCore for proper analysis?		
• Are there any devices that fell off the network during the audit?		
• Are there any diagnostics generated?		
• Are there any illegal responses?		
• Are there any retries?		
• Are there any syncs?		
• Are there any sent parameters?		

Per Segment	Yes	No
Using ProfiTrace, after each OLM, repeater, hub, or permanent monitoring station:		
• Can you identify all devices in this segment?		
• Can you generate a ProfiTrace report limited to all the devices in this segment?		
• Are there any devices that have duplicate addresses?		
• Do all devices have the correct GSD files?		
• Using the bar graph, are the driver voltages for each device above 2.5V and below 7.2V?		
• Is the idle voltage of the bus at 1V?		
• Using the oscilloscope, is the waveform clear, consistent, and square?		
• Watching the waveform, are there any EMI interference apparent?		
• Are there cabling shorts or faults on the A and B-line?		
• Do any of the devices have critical I/O data or faults?		

Comments

Acknowledgements		
We hereby confirm that this site was carefully audited and that the findings listed above are accurate.		
Engineer name:	Date audited:	Signature:
Supervisor name:	Date checked:	Signature:

8. Appendix

Attach network drawings and additional documents in this section.

9. Reference Standards

Specifications	Standard
Industrial communication networks - Fieldbus specifications	IEC 61158-1:2019
Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC 61508-4 (1998-12)
Industrial communication networks - Profiles	IEC 61784-1:2019

About Industrial Data Xchange:

Industrial Data Xchange (IDX) is an Industrial and Communications Technology (ICT) Partner that provides industry-related products, services, solutions, and training. We assist you to establish, maintain and leverage connectivity within your infrastructure.

Connectivity for Business Benefit:
Address: 1 Weaver Street, Fourways, Johannesburg, Gauteng, South Africa
Phone: +27 11 548 9960 | Email: info@idx.co.za | Website: www.idx.co.za