Industrial Data Xchange

The Industrial Data Communications Experts

IDX TECHNICAL SPECIFICATIONS

PROFIBUS Fault Finding Procedures

IDXT0102, Revision 2.1, July 2023

Table of Contents

The content contained in this document is provided for educational and informational purposes. Industrial Data Xchange (IDX) attempts to ensure that this content is accurate, but it does not represent it to be error-free. IDX reserves the right to add, amend, or repeal any content at any time without prior notification.

1. Introduction

The purpose of this document is to provide readers with a technical background and insight that will help them identify and rectify common issues that affect the health of their PROFIBUS networks. This shared knowledge has been gained over many years of experience in the field carrying out network audits and troubleshooting faulty networks across many industries.

This document contains descriptions of the typical faults that can occur in a PROFIBUS network and how to go about identifying and correcting these faults. It is by no means a substitute for certified PROFIBUS training but will give the reader an idea of certain situations that can be considered as faults in their networks and a basic approach to correcting such faults. This document also contains an approach to fault finding and some general recommendations.

Many scenarios could result in network failures and as such, not every possible fault is covered in this document. We aim to help you to address the most commonly experienced issues that can occur on your PROFIBUS network.

2. Tools required

A PROFIBUS engineer is rendered blind to a network unless they have the correct tools available 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:

2.1. Anybus ProfiCore and ProfiTrace software

Often referred to as The PROFIBUS Troubleshooting Toolkit, this essential piece of equipment, ProfiCore, and related software, ProfiTrace, 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, a built-in 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's 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 the network into segments, measuring points, and linking in the appropriate devices.

2.2. Anybus Mercury tablet

The Anybus Mercury is a multi-protocol analyser. With industrial Ethernet gaining traction, it is important to have a tool available that can troubleshoot existing PROFIBUS networks as well as newly installed/upgraded industrial Ethernet networks.

The Mercury is supplied with an industrialised Windows 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, like 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.

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.

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.

2.3. Anybus ComBricks

With Anybus ComBricks you have a valuable permanent monitoring solution for your PROFIBUS networks and when combined with the Network Condition Indicator (NCI) 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 Programmable Logic Controller (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.

2.4. 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. Ensure not to accidentally remove any stranded shield cores whilst stripping the cable.

2.5. 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.

3. Common PROFIBUS specifications and standards

3.1. Cable clearances

PROFIBUS cable is sensitive to inference from high voltage cables even though certain measures (shielding, differential signals, etc.) are taken to try and mitigate these effects. As a standard, the following cable distances should be adhered to for the various categories of cable:

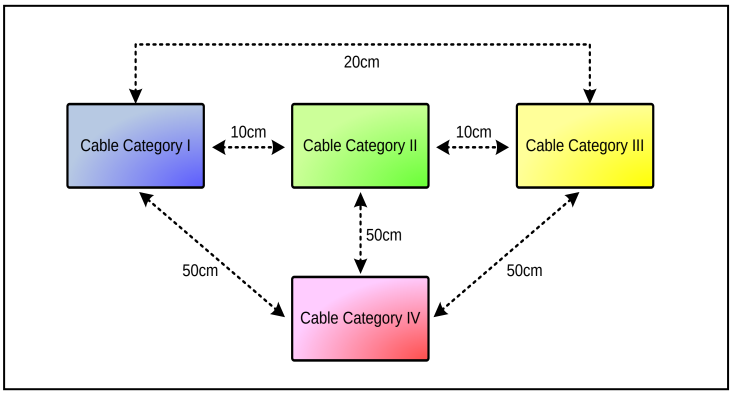


Figure 1: Cable clearance diagram by category

Category I: Fieldbus and LAN cables (E.g., PROFIBUS, AS-i, Ethernet, etc.), shielded cables for digital data (E.g. Printer, RS232, etc.), shielded cables for low voltage (< 25 V) analogue and digital signals, low voltage power supply cables (< 60 V), coaxial signal cables. Potential equalisation cables between cabinets.
Category II: Cables carrying DC voltages > 60 V and < 400 V, cables carrying AC voltages > 25 V and < 400 V.
Category III: Cables carrying DC and AC voltages > 400 V, telephone cables.
Category IV: Cables of categories I to III are at risk from direct lightning strikes (E.g., Connections between components in different buildings).

3.2. Terminations

The beginning and end of the cable must be terminated, or it will cause signal reflections on the cable that may result in intermittent failures on the bus. If the termination occurs before the end of the cable, the devices after the termination will be lost when using modern connectors.

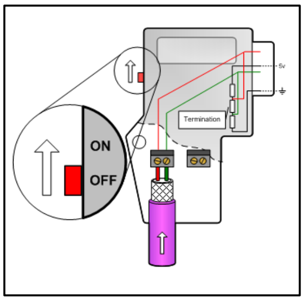


Figure 2: Termination on a connector

It is advisable to have Active Terminators installed at the ends of the segments so that the last device (usually responsible for providing the termination) can be replaced/allowed to fail, without affecting the rest of the network. A termination is a resistor circuit that requires 5V. A termination on a connector that is enabled, but not powered (by the device it is connected to) is not terminating.

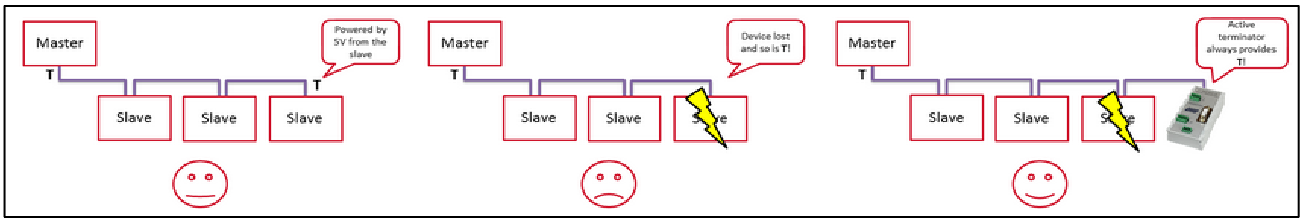


Figure 3: The difference between using an active terminator and terminating using modern connectors

Additional note: Wherever a single wire enters a connector, the cable should always be wired into the ‘incoming’ port and not the outgoing, as the outgoing port is usually disconnected once the termination switch is enabled.

3.3. PROFIBUS connector wiring standards

When wiring into a PROFIBUS DP D-sub connector the following guidelines should be considered:

- Ensure continuity of the PROFIBUS shield in each connector. The shield helps to catch and drain any EMI picked up in the field and within the electrical panels to a functional grounding point, thus protecting the PROFIBUS cores (signal) from interference.
- Ensure proper clamping of the purple cable covering within the connector.
- There is a specific slot within a D-sub connector that allows "clamping/biting" on the cable outer sheath, this is important for tension control and for providing a secure connection between the cable and the connector.
- Fast-connect plugs feature insulation displacement technology.
- This means that when the plug is clamped closed, the displacement blades automatically connect to both the A & B PROFIBUS copper cores. The cores going into the connector should **NOT** be stripped as this will prevent a proper and secure connection to the cores.
- Be very careful to not create a wire short (shield to A/shield to B) within the connector. Keep the shield strands neatly away from the insulation displacement blades.
- The use of a PROFIBUS cable stripping tool is very advantageous over a standard Stanley knife, as it allows for precise stripping measurements and adheres to consistent depth cutting without damaging the cable shield or inner cores.

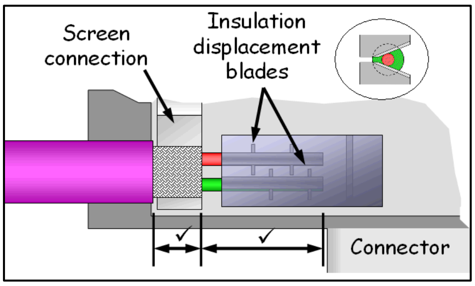


Figure 4: Guide for wiring into a Profibus DP connector

3.4. Functional bonding and shielding

There are six recommendations suggested for implementation within a PROFIBUS network to protect the network from EMI and earthing-related problems:

1. Provide both protective equipotential bonding and functional equipotential bonding through a Common Bonding Network (CBN).
2. Preferably use a 230/400 V power supply using a TN-S system.
3. Use a CBN. Mesh equipotential bonding systems as finely as possible (MESH-BN).
4. Provide a connection of the PROFIBUS/PROFINET cable shields through the housings of the connectors and the housings of the devices and thus to the CBN at each cable end with big contact surfaces (low impedance).
5. Motor cables and grounding:
    - Use shielded motor cables following the manufacturer's specifications and provide for a large-surface connection of the shield at each end to the CBN with low impedance.
    - Connect the motor to the CBN.
    - If not excluded by the manufacturer of the frequency converter, preferably use symmetrical shielded three-wire motor cables with separate protective conductors.
6. DC power supplies:
    - Multiple connections of 24-V supply circuits to the CBN must be avoided.
    - To keep the cables between the power supply unit and the consumer as short as possible, it is recommended to use several smaller power supplies rather than a single big one.

These recommendations are referenced from: *"Functional Bonding and Shielding of PROFIBUS and PROFINET - PROFIBUS Nutzerorganisation e.V. - 8.102."*

3.5. Segment cable lengths

PROFIBUS segments are limited in cable length depending on the baud rate (network speed) chosen. You should never exceed the segment length.

Repeaters will allow for the extension of the network as they boost and clean up the signal that is passed through. If long distances are required, fibre optic implementation should be considered. The table on the right shows the maximum segment lengths that can be utilised based on the baud rate.

There is also a minimum cable length of one meter that must be utilised between any two devices on the same segment on networks running 1.5Mbit/s and faster.

Baud rate	Max segment length
9.6 Kbit/s	1 000m
19.2 Kbit/s	1 000m
45.45 Kbit/s	1 000m
93.75 Kbit/s	1 000m
187.5 Kbit/s	1 000m
500.0 Kbit/s	400m
1.5 Mbit/s	200m
3.0 Mbit/s	100m
6.0 Mbit/s	100m
12.0 Mbit/s	100m

Figure 5: Recommended segment length per network speed (baud rate)

3.6. Number of devices

PROFIBUS and other RS-485-based systems are limited to a maximum of 32 devices with RS-485 interfaces per segment. Segments are separated by devices called repeaters or Optical Link Modules (OLMs). If more than 32 devices are required on a network, the network would need to be split into multiple segments, with each segment containing less than 32 devices (repeaters and OLMs are included in the count of devices as they have RS-485 interfaces).

3.7. PROFIBUS addresses

There are 128 configurable addresses on a PROFIBUS DP network (0-127), however, not all of these can be assigned to PROFIBUS devices as there are 3 reserved addresses and additionally, each network will have at least 1 master used to control the communications (request/response protocol).

The reserved addresses on a PROFIBUS DP network:

0 - Class 2 master (diagnostic and configuration tool).
126 - New device default address. PROFIBUS components are often shipped from the factory with the default address of 126.
127 - Reserved as a broadcast address.

Each PROFIBUS device should be assigned to a unique PROFIBUS address on the network (1-125), no two PROFIBUS devices can share the same address. Addresses are either configured through proprietary software, physical switches on the devices, or over the PROFIBUS network. Masters should have low addresses like 1,2 or 3 and slave devices should be addressed sequentially away from the Master.

Standard repeaters, OLMs and couplers are transparent, they do not have a PROFIBUS address, however, they do count towards the 32 devices with an RS-485 interface limit on a PROFIBUS DP segment as it is based on the RS-485 standard.

So, if a segment is cabled between 1) a Master and Repeater or OLM or 2) between two Repeaters or OLMs or 3) between a Master, Repeater or OLM and an Active Terminator in each case two RS-Interfaces are already present on the segment allowing for only an additional 30 devices.

It is also good practice not to fill the segment to allow for the addition of future devices and allow for the use of diagnostic tools such as ProfiCore. Thus, it is recommended to limit the additional devices to between 25 and 28.

4. Common faults and how to identify them

4.1. Terminations

Incorrectly set terminations are the number one cause of faults and failures within PROFIBUS networks. It is critical to understand the function of termination within a network and in what cases it should / should not be enabled.

1. Firstly, you should always have only two terminations in each segment. The terminations should always be enabled at the beginning of the segment and the end of the segment (where the bus ends), this may also be at an OLM or repeating devices.
2. Secondly, if the termination is enabled on a PROFIBUS DP connector, the connector must always be plugged into a **powered** device as the termination circuit within the connector gets its power from the device that it is connected to.

Below are some of the common PROFIBUS termination faults that can occur, and how to identify them:

4.1.1. Missing termination

As two terminations are required on each segment, a missing termination is simply where termination has not been enabled at one or both ends of the segment.

A missing termination results in reflections. A reflection is where the transmitted signal on the bus has nowhere to go (unable to be absorbed by a termination circuit) and bounces back down the bus cable causing interference and intermittent communication failures.

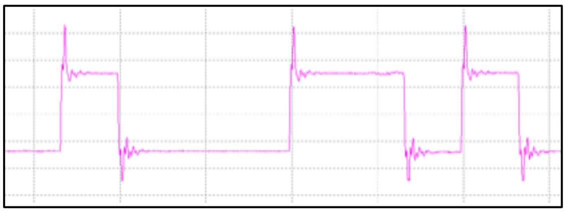


Figure 6: Missing termination waveform graph

Symptoms of a missing termination

- Oscilloscope: Increased signal amplitude and excessive ringing /reflections on the oscilloscope image.
- Voltage level: Increased driver voltages (amplitude of between 7 – 10 V are often detected).
- Device behaviour: Intermittent failure, loss of devices on the bus.

Corrective action

- Enable the termination at the beginning and end of each segment.
- Ensure both terminations on each segment are powered by the device that it is connected to.

4.1.2. Over termination

Over-termination results from enabling more than two terminations on a single segment. Over terminations negatively affect the PROFIBUS network as the extra resistance introduced into the bus affects the impedance of the segment and causes decreased signal strength across the bus as well as reflections/ringing on the scope waveform.

Over-terminations are very commonly enabled on VSDs and soft starters, as these often have integrated termination circuits (with a switch) built into the device.

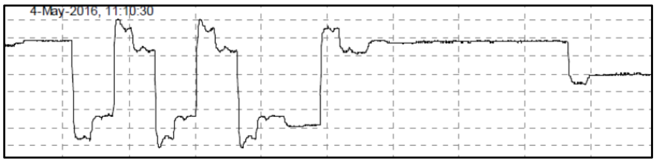


Figure 7: Oscilloscope graph for when there is over termination

Unknowingly, the technician accidentally leaves this termination switch on where it should be disabled. Thus, if you notice the symptoms that lead you to suspect an over-termination, the first place to check is at the VSDs and soft starters within the affected segment.

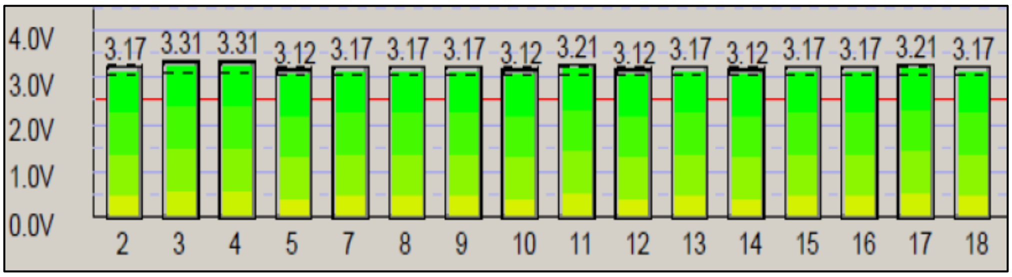


Figure 8: Segment electrical health analysis

Symptoms of an over termination
• Oscilloscope: Decreased signal amplitude and excessive ringing/reflections on the scope image. • Voltage level: Decreased driver voltages (amplitudes of between 2 – 4 V are often detected). • Device behaviour: Intermittent failure, loss of devices on the bus.
Corrective action
• Remove the over-termination within each segment. • Ensure both terminations on each segment are powered by the device with which it is connected to.

4.1.3. Unpowered termination

Even if terminations are enabled at the correct places on each segment, if the termination is unpowered then it is as if the termination does not exist. A PROFIBUS active termination circuit requires 5 VDC to operate correctly.

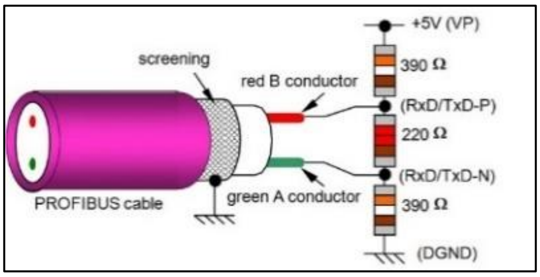


Figure 9: Active terminator

The 5 VDC comes from the device that the PROFIBUS connector is connected to. Therefore, if the device is powered down or locked out for whatever reason, the termination will lose power and not operate effectively on the segment.

You can avoid accidental unpowered terminations by effectively utilising an Active Terminator on your network.

An Active Terminator takes in 24 VDC (usually supplied by a UPS or dedicated power supply) and supplies a dedicated termination to the bus end.

Symptoms of an unpowered termination
• Oscilloscope: Increased signal amplitude and minor ringing/reflections on the scope image. • Voltage level: Lower idle voltage (Idle voltage should be at 1V). • Device behaviour: Intermittent failure, loss of devices on the bus.
Corrective action
• Ensure both terminations on each segment are powered by the device that it is connected to. • As a preventative measure, install an *Active Terminator* on each of your segments.

4.2. Wiring short circuits and cable faults

The two main causes of short circuits and wiring cable faults within PROFIBUS networks are:

1. Poorly wired PROFIBUS connectors
   - It is common to find short circuits between the A and B cores and the shield within connectors as the cable shield contains fine strands that can often creep into the terminal blocks if you are not careful.
   - A-short and B-short circuits are common where the line does not make proper continuity with the connector terminals (screw-type and fast-connect).

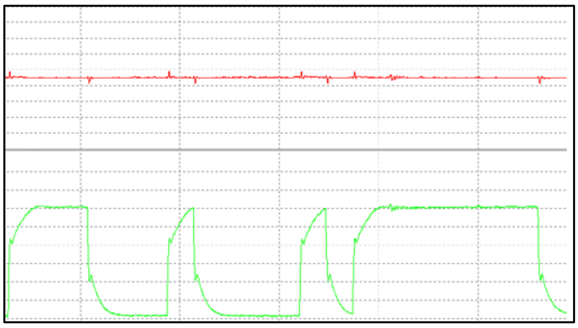


Figure 10: short-circuited A and B-line

2. PROFIBUS cable being damaged within the field
   - Commonly, cables are pinched and squashed within runs throughout the plant.
   - Cables should be properly protected from physical damage and environmental elements as they run between panels and buildings and kept off the floor to prevent accidental damage.

Symptoms of a wiring fault (short circuit/cable fault)

- Oscilloscope: Severe ringing and distortion of the scope image when connected to the affected segment. If a short circuit is suspected, identification is done by looking for a flat line on the scope waveform of the individual cores (A & B line).
- Voltage level: The voltage levels of the affected segment will be excessively low (< 2.5 V).
- Device behaviour: Intermittent illegal messages, and sporadic devices lost within the affected segment and network.

Corrective action

- Once a wiring fault is suspected, the most effective way to identify the problem device/segment is by cable isolation.
- Cable isolation identification can be achieved by connecting the bus monitor at the beginning of the affected segment and disconnecting different sections of the segment (moving from the last device towards the beginning of the segment) whilst monitoring the bus monitor for when the fault disappears. Once the fault disappears, scrutinise the previous section.

4.3. Electrostatic and electromagnetic interference

Electrostatic interference is caused by high-voltage power cables running close to the PROFIBUS cable and components. Electrostatic interference injects noise onto the PROFIBUS signal and can interfere with telegrams travelling on the bus.

Electromagnetic interference is caused by noisy devices such as VSDs or motors that create large magnetic fields.

Electrostatic and electromagnetic interference can be reduced by moving the cable and network components away from sources of interference, by the required separation specifications as per section *3.1. Cable clearances.*

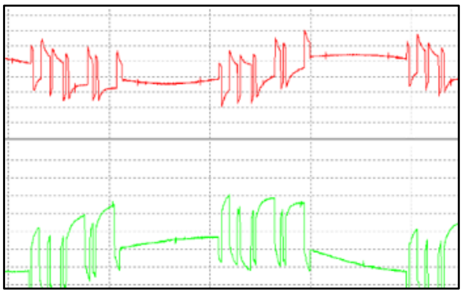


Figure 11: Signs of an EMI on the A and B-line

Figure 12: Cause of interference

Additionally, proper shielding and grounding mechanisms must be implemented across the entire network and network environment as per section *3.4. Functional bonding and shielding*.

Symptoms of electrostatic/electromagnetic interference

- Oscilloscope: Excessive ringing/noise on the scope image, unstable signal waveforms.
- Voltage level: Minor jumping of the voltage levels may occur.
- Device behaviour: Intermittent failure, loss of devices on the bus, continuous illegal messages.

Corrective action

- Ensure proper cable separation requirements are adhered to. Move PROFIBUS cables away from high voltage cables/sources of interference, this may necessitate running the PROFIBUS cable around the inner frame of the cabinets.
- Incorporate isolation mechanisms, such as OLMs, that are not susceptible to the effects of electrostatic or electromagnetic interference.

4.4. Duplicate address

PROFIBUS shares a common bus (even between multiple interlinked sub-networks). This common bus means that there is no physical message routing and that any telegrams sent out, are shared across all segments.

PROFIBUS utilises addresses so masters can communicate with slaves and vice versa. The PLC and all useful IO devices, drives, etc. (slaves) on the network are assigned a unique address. The usable addresses in PROFIBUS are addresses 1-125 (0,126 & 127 are reserved addresses and cannot be assigned to any devices).

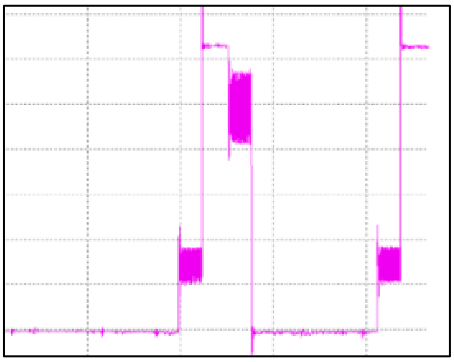


Figure 13: Identifying a duplicate address

A duplicate address is where you have more than one device on a network with the same PROFIBUS address. Duplicate addressing causes severe network failure due to collisions and duplicate telegrams travelling on the bus.

The message trace will likely show Syncs, Repeats, and Illegal messages. Syncs on “missing” devices based on the address(es) programmed into the PLC. Repeats and Illegals on the address are duplicated.

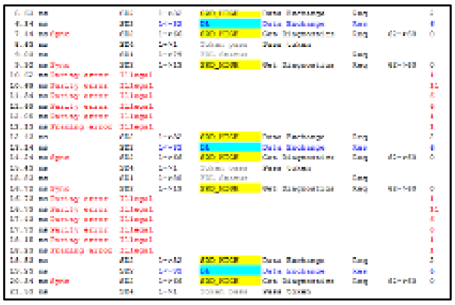


Figure 14: Messages recorded with duplicate addresses

Another way to see a duplicate address is via the bar graph of the voltage levels of the affected address with a jump up and down cyclically.

Symptoms of a duplicate address

- Oscilloscope: Severe ringing and distortion of the scope image when connected to the affected segment.
- Voltage level: the voltage levels of the affected address jump up and down cyclically.
- Device behaviour: Devices at the duplicate address are intermittently lost, and the entire bus may experience intermittent failure.

Corrective action

- To identify a duplicate address, unplug the suspected device to see if the fault disappears (and to see if this disconnected device’s address remains on the bus). To correct a duplicate address, ensure all devices on the network have a unique address.

4.5. Long segment length

There is a limit to the maximum amount of cable that can be used within a single segment on a PROFIBUS DP network. The maximum length per segment is dependent on the baud rate. The faster the network speed, the shorter the allowable segment length. See section *3.5 Segment cable lengths* for the maximum segment length allowances based on the baud rate.

Segments are linked together by utilising **repeaters** and/or **optical link modules** to build an entire network. Repeaters and optical link modules isolate adjoining segments, replenish signal amplitude (driver voltage levels), and smooth out signal waveforms within a network.

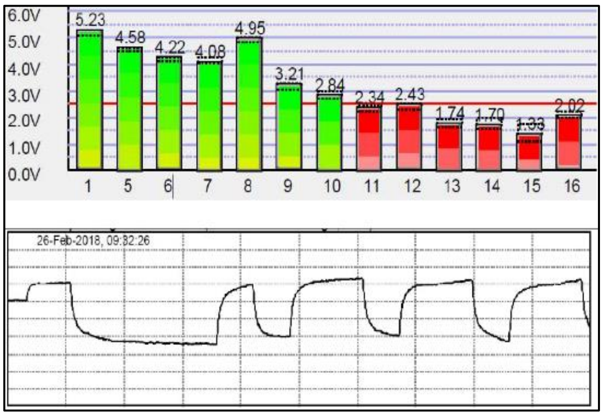


Figure 15: Changes in voltage levels on a long segment

Symptoms of exceeding segment lengths

- Oscilloscope: Decreased amplitude, shark-fin effect on the leading edge of the scope image.
- Voltage level: Decreased voltage levels towards the end of the segment (< 2.5 V).
- Device behaviour: Intermittent failure, loss of devices on the bus, network risk.

Corrective action

- Adjust the network topology to adhere to the maximum required segment lengths. Consider installing repeaters and OLMs to extend networks and allow for long cable runs between substations and plant areas.

4.6. Too many devices on a segment

The RS-485 specification and inherently the PROFIBUS DP specification limits the maximum number of devices that can be connected within a single segment to 32 devices. The 32-device limit includes a count of all PROFIBUS slaves, masters, and network components installed within a single segment or continuous run of copper cable.

Repeaters and OLMs can be used to create additional segments, therefore, allowing for more devices to be installed within a network. As a rule of thumb, network designers and installers should try not to exceed 25 devices per segment. By limiting your segments to 25 devices you allow for future expansion and place less risk on the segments during general operation.

Figure 16: Device limit

Symptoms of exceeding maximum devices per segment

- Oscilloscope: Decreased amplitude, shark-fin effect on the leading edge of the scope image.
- Voltage level: Decreased voltage levels across the entire segment (especially on the devices furthest from your testing tool connection point).
- Device behaviour: Intermittent failure, loss of devices on the bus, network risk.

Corrective action

- Adjust the network topology to adhere to the maximum number of devices per segment. Consider installing repeaters and OLMs to increase the number of network segments to allow for fewer devices per segment.

5. Fault Finding

While it is possible to generate guidelines on symptoms that indicate potential faults, successful fault finding is more dependent on:

- Intelligent application of one’s knowledge of how PROFIBUS works and what the standards require for it to work correctly.
- A sound fault-finding strategy - how we go about finding faults.
- The availability and effective use of diagnostic tools.

It is important to understand that there is no holy grail tool or person that will be able to tell you exactly what the problem is without thinking or following some form of analysis.

5.1. Preparation

The effort and time required for troubleshooting can be reduced through preparation. Preparation is a key aspect of aiding and improving fault finding. The more one knows about one’s network upfront the better position one is in when a fault occurs as one understands the network topology and has baselined the network by analysing its various segments.

Preparation is a site-wide effort and needs to be supported by management, engineers, and operators. This preparation should be done ***before*** a network failure. Preparation is an ongoing process – one needs to stay up to date for it to be effective.

Preparation includes:

- Making sure that detailed, up-to-date network diagrams are available – makes locating a problem in a PROFIBUS network simpler for both onsite personnel and contractors.

Physical familiarity with the network:

- Check every device on the network drawings can be found.
- Ensure the drawing accurately represents the bus/cabling as it is currently being used.
- Examine every device that is plugged into the network and check that you are familiar with it, what it does, how it works, what can be changed on it, how to set the PROFIBUS address and if/where to find spares.
- Note any places in the network that break installation rules. Although you may not be able to take any action while the network is running, these should be corrected during a shut.
- Make sure that you know where the terminations are and check that they are correctly set *and* powered.
- Become acquainted with all the PROFIBUS test equipment available (if there is none some should be purchased). Read the documentation to understand the tool’s uses, limitations, and how and when to use it.
- Attempt to find out how the system is programmed to act in various failure scenarios.
- What happens when a device fails?
- Under what conditions the controller is programmed to switch to clear mode/stop.
- Determine whether the PLC/ Supervisory Control and Data Acquisition (SCADA) has a diagnostic log and how to get access to it when needed. This log often contains the most recent faults experienced by the controller and is a quick way to the source of many problems.
- If you will not have direct access to this information, make sure that the operator will know what you are asking for when you request this information from him.

5.2. Common Mistake

A common mistake made when trying to solve a fault is to act without a strategy. This usually entails panicked modification of the system to get it running without an understanding of the problem.

Even if this approach works, it is difficult to trace the initial failure and the root cause has not been corrected and will likely result in further problems in future.

5.3. Structured Approach

One should take a structured approach to solving the problem. This involves ***preparation***, ***step-by-step problem analysis***, ***cause elimination*** and finally ***corrective action***.

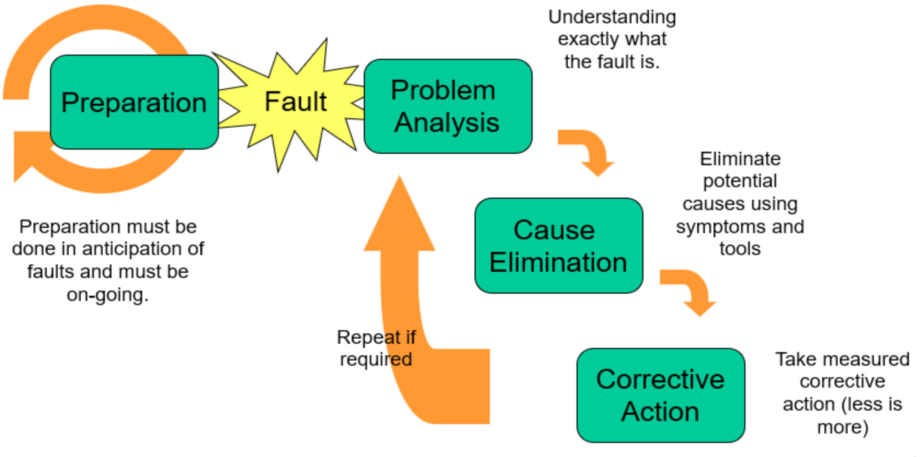

Preparation
Fault
Problem Analysis
Understanding exactly what the fault is.
Cause Elimination
Eliminate potential causes using symptoms and tools
Corrective Action
Take measured corrective action (less is more)
Preparation must be done in anticipation of faults and must be on-going.
Repeat if required

Figure 17: A problem-solving approach

5.3.1. Start at the SCADA or control room

The best place to start fault finding is at the SCADA or the controller hardware configuration with the help of operators or engineers:

- What has happened on the network – is it a single device error or multiple device errors that have caused the system to stop?
- The SCADA should be programmed to tell you which device(s) and what problem(s) were experienced (but this is usually not the case).

5.4. Problem Analysis

5.4.1. Fault Categories

To aid in troubleshooting and identify what to look for, potential faults can be categorised into three main groups:

- **Device Errors**: Physical, Process & Maintenance Alerts, Damaged Interfaces
- **Transmission Errors:** Termination, Cable damage, Cable type, Addressing, Interference, Device interfaces, Power Supplies, Earthing
- **Programming Errors:** Bus Timing, Software Configuration

5.4.1.1. Device Faults

- Device faults are things that may go wrong on a *specific device*.
- PROFIBUS provides a diagnostic mechanism whereby a device may report what has gone wrong to the master station (if this is still possible). The master station can then be programmed to take action if required.

5.4.1.1.1. Physical Faults

- Physical faults are faults that occur with the actual device hardware, such as modules.
- Physical faults can range in severity from a disconnected or broken output line to damaged modules that may need to be replaced.
- Physical faults that don’t interfere with bus communications but cause the sensor to take incorrect measurements and possibly negatively affect production are difficult to detect.

- It is up to the device manufacturer to provide mechanisms for identifying these types of errors - the most effective option is to identify the error and report it to the master station via the PROFIBUS diagnostics mechanism.

5.4.1.1.2. Process Alerts

- Process errors are not errors with the physical PROFIBUS system, but alarms fed back from a device when some variable that is being measured moves over a high-high, high, low, or low-low threshold.
- This indicates that something in the process is out of range and must be corrected or that the measuring device is incorrectly calibrated.
- It is possible for a device to raise a non-urgent alert indicating that it needs recalibration or maintenance attention.

5.4.1.1.3. Interface Faults

- Electrical problems on a device's PROFIBUS interface will prevent a device from reporting faults to the master.
- It may return incorrect data, stop communicating completely or interfere with communication on the bus.
- If the interface is damaged the device may fail and prevent bus communications (e.g.: short circuit).
- Common reasons for electrical faults on devices:
    - Power surges or lightning strikes
    - Incorrect device installation
    - Overheating

5.4.1.1.4. Device Faults Summary

- Physical inspection of the device after examination of SCADA information will often reveal a fault.
- Take note of the state of the LED lights on devices. The device manuals will often give tables to decode faults based on the state of the LEDs.
- Analysis of the electrical signals generated by the device is required to tell if the interface is working correctly (the best is an oscilloscope).
- Note how many devices are affected and do they have anything in common: Multiple devices on the same segment usually indicate transmission faults.

5.4.1.2. Transmission Faults

A **transmission fault** occurs if a PROFIBUS message or packet placed on the bus does not reach its destination or becomes damaged along the way.

The possible causes for a transmission fault are numerous but usually have characteristic behaviour that affects multiple devices. This makes it simpler to identify them.

Symptoms are typically:

- sporadic device and/or segment operation
- total segment failure

Typical transmission faults include:

5.4.1.2.1. Termination Faults

- If a copper segment is not terminated or is over-terminated, signal reflections on the cable may interfere with the successful transmission of PROFIBUS messages.

5.4.1.2.2. Cable Damage/Faults

- Breaks in the cable, A or B lines or twisting A-B can result in failed communications.
- Often less obvious is that significant distortion of the cores may lead to reflections which will upset bus communications.

5.4.1.2.3. Cable Type

- Using a cable that does not match the PROFIBUS specifications will result in unreliable communication with the most unpredictable symptoms.

5.4.1.2.4. Address

- It is common for two PROFIBUS devices to be accidentally configured for the same address.
- As both will attempt to respond at the same time to messages from the master station, there will be a “collision” of electrical signals on the bus.
- In most cases, the master will not be able to communicate with either device.
- Due to delays in the response times of some devices, one or both devices may occasionally successfully respond and “flash on and off” in the SCADA, Hardware Configuration Tool, or live list.

5.4.1.2.5. Interference

- When PROFIBUS messages are corrupted by electrostatic or electromagnetic interference the results are unpredictable network operation.
- If the interference is permanent, communication may be erratic or completely disrupted presenting similar symptoms to a termination error.
- When the interference source is only triggered by a particular event, like starting a large VSD or furnace, the result may be sudden unexpected bus trips.
- Best detected with an oscilloscope.

5.4.1.2.6. Power Supplies

- If a PROFIBUS DP device cannot supply sufficient power to its bus driver interface, then the signal that it transmits down the bus may be faint or unclear.
- This is commonly seen when powering multiple devices off a single power supply or when using devices that have heavy consumption (e.g.: radio transmitters).
- It can also be a problem where remote IO devices have many IOs all drawing power from the same supply as the interface unit.
- Remote IO devices provide the option of powering the device interface from a separate power supply to prevent rush currents from interfering with bus communications and to allow the head unit to operate even if there is a short on one of the IO loops.
- On PROFIBUS DP the strength of the signal on the bus can be measured (with an oscilloscope) as the voltage difference between the peaks and troughs of the differential signal (B-A).
- If this value starts to degrade or is found to be very low (2.5 – 7.2V limit range), a power supply issue should be suspected (after over-termination, cable length/type has been ruled out).
- PROFIBUS PA suffers from similar power problems if the power supply connected to the coupler is insufficient or the PA device demand is too high.
- A non-EEx coupler can supply 400mA to devices on the MBP segment. Designers must ensure that the devices they install will not ever have a combined consumption of more than the coupler maximum.

5.4.1.2.7. Earthing

- Earthing is frequently neglected in PROFIBUS installations and can result in sporadic problems due to interference.
- Ensure the screens in the plugs are properly connected so that the shield is continuous.
- Cables should be earthed where they enter and exit the cabinet directly to the cabinet or cabinet earth bar.
- The effectiveness of the earthing is best measured with an oscilloscope when the network is silent (i.e.: not running).

5.4.1.2.8. Transmission Fault Summary

- Transmission faults can be difficult to diagnose because you are dealing with a sensitive, high-speed electrical system.
- Proper test tools that analyse and can “talk” on this system are invaluable to finding faults quickly and accurately.

5.4.1.3. Program Faults

Program or Configuration Faults are not usually the domain of maintenance personnel, but it is good to be aware of them.

When all other potential problems have been exhausted it may be time to call on the software engineer to investigate and adjust some of his settings that may be causing network problems.

5.4.1.3.1. Timing Faults

- PROFIBUS operates under very strict timing constraints setup within the master station - if these are disobeyed the network will fail.
- One such constraint is the slave **Watchdog Time**. As a safety measure, if a slave on the network does not receive communication within this time it registers a bus fault and switches to a “failsafe state”.
- If this timer is set too short, devices may register bus failures during normal operating mode even though the network is operating correctly.

5.4.1.3.2. Software Faults

- Programming errors can either prevent the controller from starting or cause it to fail under certain conditions.
- Most controllers will indicate the type of error with LED lights on the faceplate.
- If the controller is indicating a program stop rather than a communications error, this may solve troubleshooting time.
- Program stops may be caused most commonly by invalid memory accesses or invalid operations (i.e. divisions by zero).
- Understanding the master-slave operational cycle when the system starts and operates is very useful for fault-finding system configuration/parameters or other advanced faults.
- Certain diagnostic test tools/software, like ProfiTrace, allow you to examine where in the cycle a device is and also examine what data is being passed between the master/slave.

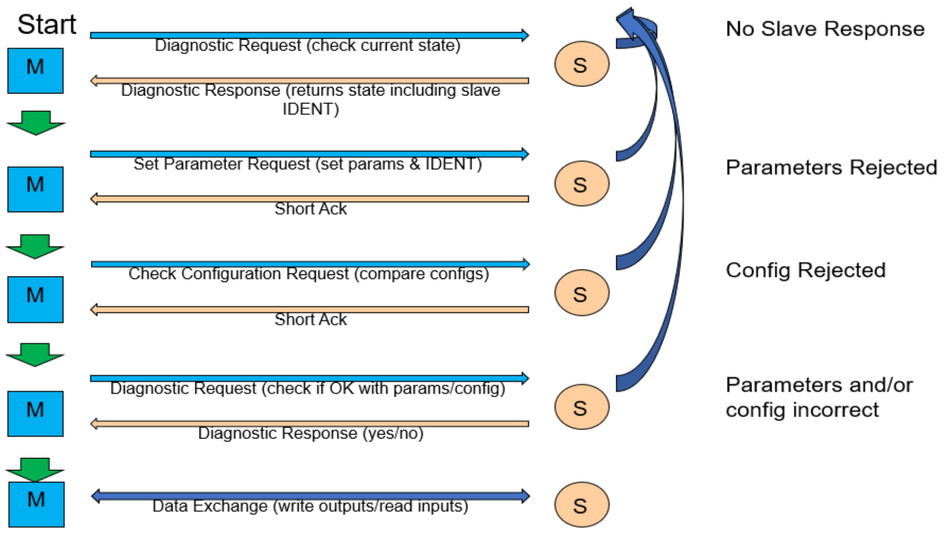

Start
M
Diagnostic Request (check current state)
Diagnostic Response (returns state including slave IDENT)
S
No Slave Response
M
Set Parameter Request (set params & IDENT)
Short Ack
S
Parameters Rejected
M
Check Configuration Request (compare configs)
Short Ack
S
Config Rejected
M
Diagnostic Request (check if OK with params/config)
Diagnostic Response (yes/no)
S
Parameters and/or config incorrect
M
Data Exchange (write outputs/read inputs)
S

Figure 18: System start-up process

5.4.1.3.3. Program Faults Summary

- Although it may be tempting to blame any faults on software/programming, these are only most likely during/soon after commissioning.
- If the system has been running without fault for some time the software is unlikely to be the cause of a fault and a thorough check for device and transmission errors should be checked first.
- Where communication between a master and slave is operating correctly but the data appears incorrect, this is almost certainly a programming error.

5.5. Test Tools

Just as one would not expect a mechanic to be able to fix a vehicle fault without looking under the bonnet and without the correct tools, we cannot find faults quickly and accurately on PROFIBUS proper tools.

A multi-meter is **not** a PROFIBUS DP diagnostic tool (because the system is digital and high-speed). It is however useful for power/voltage measurements & checks on PROFIBUS PA/ASi.

5.5.1. Cable Testers

Tools that are capable of testing the physical wiring of the network are referred to as Bus or Cable Testers and will typically test:

- cable shorts and breaks
- check the network termination
- report the cable line lengths
- Report cable impedance properties

Advanced bus testers will also allow scanning any attached devices to report their respective signal strengths, capture error messages and bus statistics or even configure and control individual stations.

5.5.2. Signal Testers

The fact that a system is working is not a good indication of the system’s health!

A far better idea of potential bus problems must be based on the shape of the electrical signal waveform. This can only be observed using a high-speed oscilloscope.

If the waveform appears as a neat square wave this means that the cable installation is well implemented. If not, then this will indicate a less healthy system that may give trouble sometime in the future.

The amplitude (height) of the square wave needs to be, at minimum, 2.5V for operation in noisy industrial environments.

Lots of oscillation (instability) in the signal usually indicates excess cable capacitance or faulty termination (best seen while the network is running) while erratic hum and occasional spikes are produced by coupled-in interference (best seen with the network stopped)

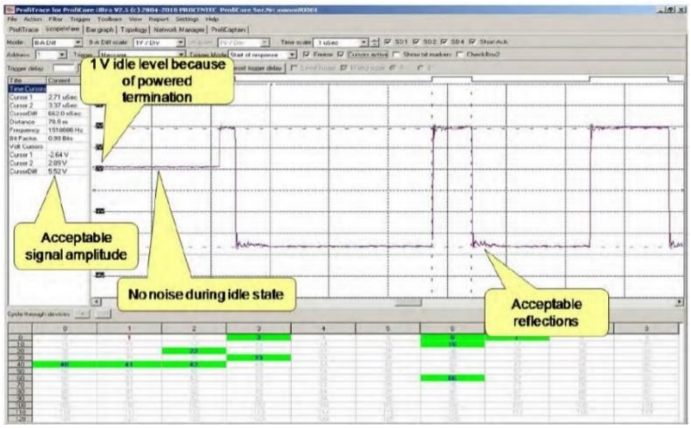
5.5.2.1. Oscilloscope

The scope used should have 2 channels, be able to display the A-B signal differential and have a bandwidth of 100Mhz. Being able to record values over some time and upload these to a computer is also extremely useful.

Connecting the scope to the network requires an access point where the probes can be connected to the data lines

This is most effectively achieved where the cores are exposed at a repeater or by plugging a specifically built-up connector into a piggyback plug.

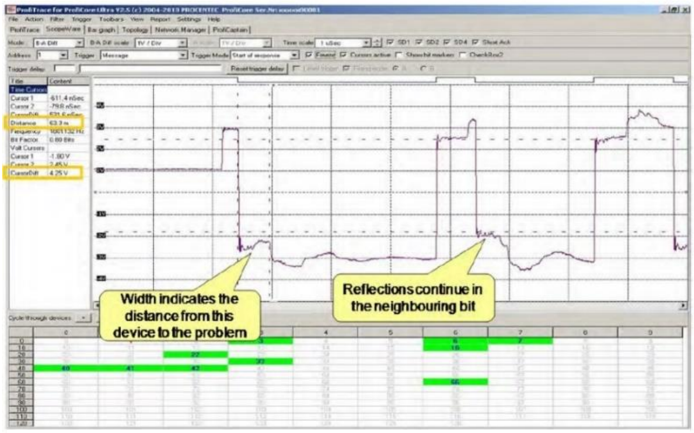
5.5.2.1.1. Acceptable Signal



1 V idle level because of powered termination
Acceptable signal amplitude
No noise during idle state
Acceptable reflections

Figure 19: Oscilloscope reading for an acceptable signal

5.5.2.1.2. Wire Break or Termination Error



Width indicates the distance from this device to the problem
Reflections continue in the neighbouring bit

Figure 20: Oscilloscope reading when there is over termination

5.5.2.1.3.EMC / Noise

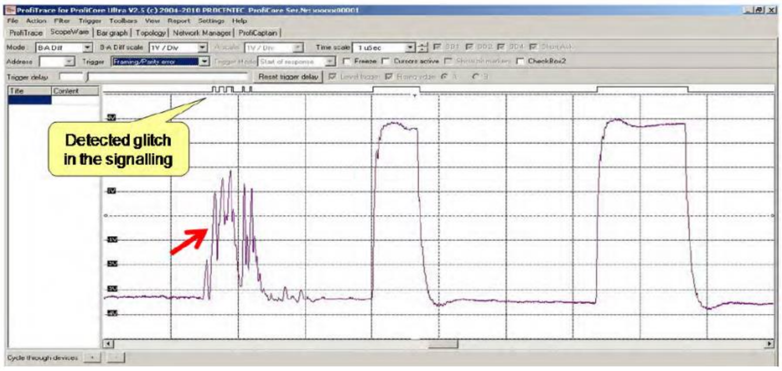


Figure 21: Oscilloscope reading when there is noise on the network

5.6. Cause Elimination

To eliminate a fault, we should ask what the fault symptom is. We define categories to examine possible fault types, causes and fault escalation.

Assess if the fault is affecting one device, multiple devices but not all in a segment, all devices in a segment, all devices after a certain point or device, multiple network segments, the whole network, or even multiple networks.

In the rare case of multiple networks, it is likely something common to the networks like a power supply or UPS and not a fault on any of the individual networks.

Assuming the fault or faults are limited to a single network we would work through the following procedure:

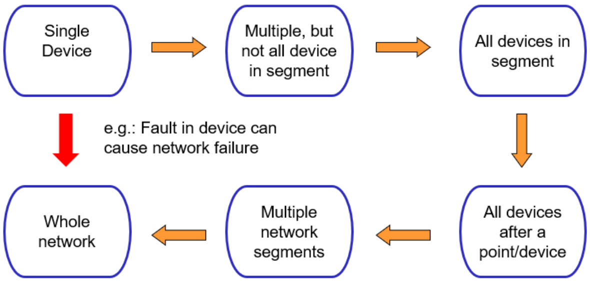

Single Device
Multiple, but not all device in segment
All devices in segment
e.g.: Fault in device can cause network failure
Whole network
Multiple network segments
All devices after a point/device

Figure 22: Fault finding and elimination procedure

5.6.1. Single Device Affected

- Check whether the communication is still available – if you can still "talk" to the device (such as see it on a live list) there is a device fault, such as a faulty module or configuration.
- If the device is not communicating, physically verify that the device is connected, and powered.
- Check that the device address matches that set in the master configuration. Remember that PROFIBUS addresses are only updated after the device has been turned off and back on; so power cycle the device before returning from the field.
- Make sure that there is not a duplicate address by connecting a tool that can generate a device live list and checking if the address is still on the bus after you unplug the faulty device.
- Check that the device signal voltage is in the 2.5-7.2V range. Low voltage indicates a power supply or a device interface problem. Measure the voltage on the device's power supply (24v in most cases) - if it is not the power supply the device may be faulty.
- Check that the device is well earthed to the cabinet earth (built-up charge can cause problems), and for visual signs or the smell of burning. Replace the device if necessary.

5.6.2. Multiple Device Affected

- Perform checks for single-device faults.
- If all of the troublesome devices are located in the same area or network segment, check:
  - that the cable to that segment has not been damaged.
  - that the segment terminators are on in the correct places and nowhere else.
  - that the segment repeater is working correctly.
- Connect a bus tester/analyser to the affected segment and check if it picks up the request packets from the master station. If not, there is a physical fault with the connection - use a bus tester to check the cable for faults.
- If the master is communicating but no slave responses are evident, check that all of the devices have power and are still connected to the bus.
- Use a short piece of PROFIBUS cable and try to initiate a connection to one of the devices from a handheld tester. If a response is received plug it back into the bus and connect an oscilloscope or a digital signal tester that can report the differential voltage level on the bus. If this value is low, check that the power supply is operating properly and replace it if necessary.
- If you do not get a response from a device even directly connected with a short cable, the device interface may have been damaged by lightning or a power surge.

5.6.3. Whole Network

- Check that the DP connector has not come loose from the master, that the master has power and that there are no cabling faults on the segment that the master is connected to.

5.6.4. Multiple Networks

- Check if they share a common power source or UPS and if there are issues with a reliable supply.

5.7. Fault Finding vs Audit

PROFIBUS Fault Finding is different from performing a PROFIBUS Audit which is a more detailed and time-intensive procedure. The goal of PROFIBUS Fault Finding is to find the main fault or faults stopping the network from running entirely or continuously for a long period as quickly as possible and correct them.

During the PROFIBUS fault-finding procedure, note all items that do not meet the PROFIBUS standard that should be corrected at a later stage. These may not be the specific faults causing the downtime or critical enough to warrant immediate attention and can be addressed in the future during scheduled maintenance.

It is always easier to trace a permeant fault that is preventing the network from running currently rather than an intermittent fault. Often intermittent faults need continuous logging or permanent monitoring to understand their true nature.

Assuming we are dealing with a permeant fault that is preventing the network from running currently, after gaining as much information as possible from on-site personnel regarding the fault one would want to:

1) Visually inspect the network for termination, condition of cabling and wiring of connectors, and LEDs of devices. Make special note of any Repeaters, Diagnostic Repeaters and OLMs.
2) Attach a diagnostic tool such as a ProfiTrace at the PLC and look at the live list, messages, and message statistics. Looking for obvious issues like Repeats, Illegal Responses in the messages or Syncs, Lost Stations etc in the Message Statistics.
3) Attach a diagnostic tool such as a ProfiTrace to each segment and look at the standard waveform (B-A) and the separate A & B waveforms. You are looking for a square standard waveform (B-A) and no signs of EMC / Noise or A/B to Shield shorts on the separate A&B waveforms. If the segment

looks healthy, then proceed to the next segment. Where the waveform is not nice and square further investigation is warranted.

4) Whilst attached to each segment you also want to look at the bar graphs for the devices on each segment. You want to check the voltages are between 2.5V and 7.2V per the PROFIBUS Standard but in practice ideally between 4V and 6.5V. Anything out of the range is generally worth further investigation especially if on previously generated ProfiTrace reports the device was within this range.
5) Having the relevant ProfiTrace Network Data files (*.ptn) for 3 & 4 would aid in fault-finding. Limiting the analysis to the relevant devices on each segment will greatly simplify fault finding.

6. Fault Finding Procedure

Below is a general Fault-Finding Procedure:

1. Use any information you can obtain from the SCADA/Master/PLC side to understand what device(s) were affected and where they are physically located.
2. Identify the potential faults using the table on the next page to try and narrow the possible fault causes.
3. Perform a visual inspection of the areas of the network affected by the fault to eliminate potential or obvious physical/cable faults.
    a. PROFIBUS cable near high power:
        i. PROFIBUS cable should be 10cm away from power cables that carry more than 25V AC or 60V DC but less than 400V AC or DC.
        ii. PROFIBUS cable should be 20cm away from power cables that carry 400V AC or DC or more.
    b. PROFIBUS cable bends (solid core) exceeding minimum radius:
        i. 75mm radius for a single cable loop.
        ii. 150mm radius for multiple loops.

    Open trunking to check cabling. Often 180 degrees bend within trunking.
    c. Damaged cable
    d. Grounding & shielding issues:
        i. Check for situations where the shield has been cut and only the A & B lines are wired into the terminal screws. Often present at VSDs.
    e. Poorly wired connectors:
        i. No shield should be visible outside the Sub D9 connector if it is wired correctly.
    f. 1m metre rule between devices at speeds >= 1,5Mbs.
4. Use a tool such as:
    a) Use a handheld test tool, such as the Hi-Port HP25:
        - Verify the cabling and termination integrity of every segment.

    b) Use a diagnostic tool, such as the Anybus PROFIBUS Troubleshooting Kit:
        - Check that basic communications with the device can be established (using a live list for example).
        - Ensure device signal voltages of devices, for each segment, are within acceptable ranges - this can reveal power supply/interface/cable length problems.
        - Note you can’t measure waveforms or voltages of devices not within the current segment across repeating devices e.g. Repeaters/OLMs. You simply measure the voltage of the repeating device itself.

    c) Consider using a Class 2 Master, such as ProfiCaptain:
        - To scan the network to obtain all addressable PROFIBUS devices on the network with their PROFIBUS Ident Numbers. Ideally, preload all the GSD files for the devices into the ProfiTrace GSD library on the laptop being used for fault finding.

- Ensure you select a free PROFIBUS Address for your Class 2 Master. Avoid using the current Controlling Master of the Network as this will likely trip the Network.
- Ensure your baud rate for the Class 2 Master is the same as Network to be scanned.

d) Consider using the Network Manager feature of ProfiTrace:

- Take the time to build your physical network out in Network Manager reflecting the various segments, relevant measuring point(s) and PROFIBUS devices in the various segments.
- Thus your measurements and reports are relevant to the PROFIBUS devices in the particular segment being measured.

5. Use a high-speed oscilloscope to analyse the PROFIBUS communications signals (measure the difference between B and A-lines) when:

   a) The network is silent, i.e.: the master(s) is not running. The resulting measurements reveal potential noise and grounding problems.

   b) The network is running. This illustrates the quality of the cable installation and its effect on the communications signals.

   - You are looking for a nice square waveform with sufficient amplitude (height) ideally between 4V and 6.5V.
   - Check both the B-A and A and B waveforms separately for signs of noise/EMI.
   - If the waveform has a lead edge like a shark fin, then potentially too much impedance in the segment is present potentially due to the:
     - Too long a cable length for the baud rate.
     - Too many devices in the segment.
     - Over termination.
   - Excessive high voltages for all devices in a segment (usually best seen via a bar graph) indicate missing termination.
   - Excessive low voltages for all devices in a segment (usually best seen via bar graph) indicate over-termination. Focus on devices that allow termination via dip switches like VSDs and soft starters.
   - Low voltages on one device in a segment check the device and its power supply or if it is towards the end of an excessively long segment for the baud rate.

6. After eliminating all the physical aspects of the network, the fault-finding process needs to be escalated to include the Master configuration and other high-level tools. This will usually involve a PROFIBUS Engineer to check that the:

   - Device configurations and addresses match those of the devices in the field.
   - Network master bus timing and baud rate are configured correctly in all masters and are suitable for the physical network configuration.
   - Network communications do not reveal any faults. In this case, a temporary or permanent network traffic analyser is invaluable to gain insight as to what is happening in the process of Master-Slave communications and record these communications to provide historical data that can provide clues as to events that lead to a failure that is difficult to isolate.

Faults are listed in order of priority to be checked:
V - Visual inspection is often sufficient
H - Handheld tester recommended
T - Traffic analyser recommended
O - Oscilloscope recommended
*Items require access to the master configuration.

Single device affected	**All devices affected after a point/device**
• The device is not connected to the bus. [VH] • Power supply issue. [HO] • The device is at an incorrect address. [V*] • The master configuration is incorrect in terms of the IO configuration, GSD or expected station address. [VT*] • Device module fault. [VT] • Device interface/unit fault. [HO] • The device is not a PROFIBUS device (devices marked with RS-485 interface are not usually PROFIBUS DP devices). [VH]	• Cabling fault, typically: A-B swapped A/B line broken or complete cable break. [VH] • Gateway/repeating device fault. [HT] • Terminator on at a point in cable-all devices connected to outgoing connection on plug disconnected. [VH] • Devices of the same type are all incorrectly configured or do not support the current baud rate/network bus timing. [T*] • Overloaded power supply or power supply fault if all affected devices are connected to the same source. [HO]
Multiple, but not all, devices in a segment affected	**All devices in a segment affected**
• Cabling fault, typically: segment cable too long for baud rate, A-B crossed or wrong cable type. [VHO] • Termination fault: none, only one or over-termination. [VHO] • Duplicate addresses. [VT] • Overloaded power supply or power supply fault if all affected devices are connected to the same source. [HO] • Electromagnetic/Electrostatic interference. This occurs often in cabinets where cable separation distances and grounding principles are not adhered to and/or where VSD controllers are installed. [VTO] • Cable separation distances are not applied in the segment. [VO] • Earth problems/faults. [O] • Bus timing is incorrect, especially when using multiple masters or complex repeater/fibre configurations. [TO*]	• Gateway/repeating device or interface failed (includes fibre OLM, DP repeater, PA coupler and PA link). [VH] • Incorrect gateway/repeating device configuration usage (check physical settings on the device, usually dip switches and check device manuals). [VH] • Termination fault: no, only one or duplicate termination. [VHO] • Cabling faults. [HO] • Is the master running (in the case of single-segment networks)? [VT]
Multiple network segments affected	**The whole network affected**
• Poor cable installation and ignorance of installation rules (cable type, cable lengths). [VHO] • Incorrect gateway/repeating device configuration usage (check physical settings on the device, usually dip switches and check device manuals). [VH] • Incorrect bus timing. [T*]	• Master failure. [VHT] • Master physically disconnected from the network. [VT] • Master power supply fault. [VH] • A/B swapped at the master. [VH] • Device failure causes a process failure and hence by system design, a Master stop of the network. [T] • Physical cable and related faults cause large-scale communications (and thus electrical) disruptions. [HT] • Gateway device misconfiguration cause large-scale communications (and thus electrical) disruptions. [T] • Interference/earth problems cause large-scale communications (and thus electrical) disruptions. [T] • Bus timing/parameters incorrect (multiple master systems must ensure all timings are the same on all masters). [T*]
Multiple networks affected	
• Check if the networks share a common power source or UPS and if there are issues with a reliable supply especially if a UPS is involved.	

7. Tips & Tricks

Below are several tips and tricks to aid your preparation for fault finding:

a) Simple network diagrams or at a minimum network segmentation lists documenting which devices are on which segments and which devices are Diagnostic Repeaters, OLMS, and DP/PA Couplers. Undertaking Network Scans using ProfiTrace can be some assistance in identifying what devices are present on your networks and at what addresses. Consider providing this information in a marshalling cabinet containing the PLC for each network.

b) From these network diagrams or network segmentation lists, produce ProfiTrace Network Data files (*.ptn) for use with ProfiTrace and ProfiCore for each network with at least one measuring point per segment.

c) Access to all segments of the PROFIBUS DP network. Piggyback plugs on every PROFIBUS DP segment to provide access to each segment is vital for troubleshooting. Ideally from both ends of the segment but at a minimum from the beginning of the segment. Replacement of Siemens Diagnostic repeaters with Anybus B2 or B5 ProfiHubs. A B2 ProfiHub is an almost direct replacement for a Siemens Diagnostic Repeater allowing for the main channel and two additional channels (Channel 1 & 2). The main advantage of a B2 ProfiHub is that it allows one to attach a ProfiTrace to each segment for easier analysis and fault-finding. A B5 ProfiHub can replace a Siemens Diagnostic Repeater with the advantage of five additional channels instead of just two allowing for greater segmentation of the network and therefore faster troubleshooting when faults occur.

d) Training for onsite staff on PROFIBUS, fault-finding techniques and the proper use of ProfiTrace. It is recommended that all site technicians, engineers, and contractors responsible for the maintenance and installation of the PROFIBUS networks should undergo certified PROFIBUS training, at minimum a Certified PROFIBUS Installers course.

e) Base existing networks using ProfiTrace and the ProfiTrace Network Data files (*.ptn). General baseline reports for each segment of each PROFIBUS network starting with troublesome or critical networks.

f) Consider additional labelling of PLC to indicate which network they belong to e.g., Network Name, PLC Number.

g) Consider additional labelling of marshalling cabinets to indicate which Network / PLC they belong to, which Segment they are in and if they contain an access point. E.g., Network: Pasteuriser (or PLC: 53); Segment: 1; Access Point: Yes

h) Consider additional labelling of devices to indicate which Network / PLC they belong to, which segment they are in, their PROFIBUS Address, PROFIBUS Ident Number, Make and Model.

i) Check for PROFIBUS cable for clearance violations. For example, PROFIBUS cable running near, less than 20 cm, for Category III (voltage AC & DC >= 400V) lines or near, less than 10cm, Category II (voltage AC >= 25V or DC >= 60V) lines.

j) Check PROFIBUS cable bends – Visually inspect, especially in trunking, PROFIBUS DP cables for sharp bends (180-degree U bends or tight 90-degree bends). Remove any such bends from the wiring. Re-cable if necessary.

k) 1-metre rule (>= 1.5Mbits) – identify and correct violations of the 1-metre rule usually when VSDs are close to each other. This is a less critical item and can be prioritised last and only if the network waveforms indicate it is necessary to address which often isn’t the case if only one or two violations exist per network/segment.

8. Additional steps to improve network reliability and availability

8.1. Certified Training

One of the best steps to improve your potential for high network availability, performance, and quick correction of any PROFIBUS faults that may arise, is to ensure personnel responsible for the initial installation, day-to-day maintenance, upgrades, and fault finding on the network have the necessary competence. The best way to improve personnel competence across your site and with your contractors is to implement a process of certified training on the relevant technologies.

Throughout the world, there are thirty-two PROFIBUS/PROFINET International (PITC) certified training centres that are fully qualified and capable of offering the necessary training.

The IDX Academy operates the PITC in South Africa and is fully certified to conduct the following internationally recognised certified courses:

8.1.1. Certified PROFIBUS Installer Course (with troubleshooting and maintenance module)

This course is the prerequisite for all other certified PROFIBUS courses offered and forms the basis for you to develop your knowledge of the PROFIBUS protocol. Attendees will be introduced to the concept of digital systems and be guided through PROFIBUS fundamentals, installation best practices, and sound fault-finding procedures.

A well-balanced course incorporating both theoretical learnings and practical exercises empowers students and provides them with the knowledge to confidently maintain the high availability of their PROFIBUS networks.

Everything from how to build a PROFIBUS cable, device addressing, PROFIBUS network components, troubleshooting best practices and hands-on practical exercises are covered in this 2-day certified course. The content covered in this course is fundamental for any personnel involved in installing or responsible for the general day-to-day maintenance of PROFIBUS networks.

8.1.2. Certified PROFIBUS Engineer Course

The highest level of certification is available for PROFIBUS DP. In the certified PROFIBUS engineers' course, attendees will learn all about the PROFIBUS protocol with an in-depth focus on telegrams and messaging mechanisms and will gain valuable knowledge in message decoding.

How the communication between devices occurs, the successful configuration of a PROFIBUS network, and troubleshooting with hands-on exercises using some of the many troubleshooting tools available are all covered in this 5-day certified course.

On successful completion of the course, candidates will have gained the ability to resolve even the most difficult network issues experienced across their plant/site.

8.1.3. Certified PROFIBUS System Design Course

This course is primarily aimed at persons that are involved in the design and implementation of new PROFIBUS networks. The course covers all relevant topics and imparts the knowledge required to successfully design PROFIBUS networks with a focus on installation guidelines, useful network components, and best practices to ensure that your PROFIBUS networks are designed/installed fault-free right from the beginning.

It is often the case, and from our experience from PROFIBUS audits and callouts conducted over the years, that many PROFIBUS faults are a result of poor initial network design and installation. The knowledge gained from this course will assist you with your decision-making during the network design phase as well as the successful implementation of a fault-free PROFIBUS network installation and commissioning.

8.2. Permanent monitoring

A permanent monitoring solution, such as the Anybus ComBricks, is an asset to incorporate into your PROFIBUS network installations across your site. In addition to storing a history of all events that have occurred across your network that can be later analysed to identify potential causes for network failures, a permanent monitoring solution such as this can be used to provide PROFIBUS engineers with remote access into your network without the need for costly callouts.

Because the ComBricks features a date and time-stamped network event log, it makes it that much easier to capture the point of failure and to subsequently assist in resolving intermittent network faults that are rarely captured with on-site troubleshooting tools. By configuring triggers on certain events, you can receive email notifications when a network failure has occurred or is likely to occur, think preventative maintenance!

An effective permanent monitoring solution should have the ability for constant monitoring of PROFIBUS network statistics, have mechanisms available for analysing signal waveforms and device driver voltages, be able to keep a history of network events, and offer some form of notification to relevant personnel should a potential fault-producing event be detected.

8.3. Network audit by a Certified PROFIBUS Engineer

Regular inspections/audits are the keys to maintaining the high availability of your PROFIBUS networks, and to preventing unwanted downtime that affects your production, by identifying potential problems that can be addressed and corrected before a network fault occurs.

It is recommended that a certified PROFIBUS engineer conducts an annual audit on each of your PROFIBUS networks to ensure that there is no degradation of the network's health year after year. Additionally, an audit should precede any planned network upgrades or changes to confirm that no existing problems are present on the network before the change is made.

A second audit should then be conducted after the changes have been implemented to make sure that these changes have not compromised the integrity of the PROFIBUS network. A properly conducted network audit will consist of both a visual inspection and a network check of each segment using the appropriate troubleshooting tools.

On completion of the audit, a report will be issued that summarises the overall health of the network as well as any issues identified and the corresponding corrective actions that can be taken to address these issues.

8.4. Substation and RIO-panel environmental factors

8.4.1. Temperature

Although industrial electronic components, like PROFIBUS devices, do have an extended temperature range tolerance (often -40°C to 80°C), the challenge faced is that a lot of external field instruments panels and buildings without the correct protection (cooling, shade, and heating) mechanisms in place can often exceed these ranges and tolerance.

Our experience in the field with the harsh African sun has often shown us that when a PROFIBUS device is exposed to temperatures of 50°C and higher, the device becomes a lot more sensitive to minor faults and may intermittently fail.

Here are a couple of suggestions to ensure your devices are protected from excessive temperature exposure:

- Use canopies above RIO panels in the field to cast a shadow on the box. Very often RIO panels can act like an oven and exceed temperature tolerances on a hot day.
- Put procedures, or even automated systems in place to monitor the performance of air conditioning units within substations. The procedure or system should check the room temperature and aircon states regularly and provide a mechanism for reporting any failures.
- Ensure effective ventilation and airflow of all panels within a substation.

8.4.2. Ingress Protection

Below is an IP rating table that provides insight into the protection level offered by each category:

IP	First digit: Ingress of solid objects	Second digit: Ingress of liquids
0	No protection	No protection
1	Protected against solid objects over 50mm e.g., hands, large tools.	Protected against vertically falling drops of water or condensation.
2	Protected against solid objects over 12.5mm e.g., hands, large tools.	Protected against falling drops of water if the case is disposed up to 15 from vertically.
3	Protected against solid objects over 2.5mm e.g., wire, small tools.	Protected against sprays of water from any direction, even if the case is disposed of up to 60 from vertically.
4	Protected against solid objects over 1.0mm e.g., wires.	Protected against splash water from any direction.
5	Limited protection against dust ingress. (no harmful deposit)	Protected against low-pressure water jets from any direction. Limited ingress permitted.
6	Protected against dust ingress.	Protected against high-pressure water jets from any direction. Limited ingress permitted.
7	N/A	Protected against short periods of immersion in water.
8	N/A	Protected against long, durable periods of immersion in water.

Devices installed in the field without the protection of a higher-IP-rated panel should have integrated ingress protection mechanisms. Very often devices exposed to moisture and dust require, at minimum, an IP65 rating within industrial environments.

If a higher-IP-rated panel is used in the field (RIO panel), it is acceptable to install Lower-IP rated devices within this panel. Apart from ensuring the panel adheres to the required IP level, the following factors must also be considered:

- Ensure that when plant personnel access these RIO panels for maintenance, the panels are sealed properly upon departure, especially in areas that are exposed to large amounts of dust, steam, and water exposure.
- Ensure the door and side panel seals on the higher IP-rated RIO panels are in good condition and make a consistent seal. Often the rubber seals on these panels deteriorate over time, get damaged, and require general maintenance and repair.

- Ensure all cable entrances at the base, top, and sides of the panel are adequately sealed to achieve the required IP rating for the area in which the panel is installed. Do not leave any open cable ports where dust, moisture or pests can gain access.

8.4.3. Pest and rodent protection

Rodents and pests create a large risk for PROFIBUS communication networks, and can often cause damage to cables, and devices and even create a hazard for the instrumentation and electrical personnel responsible for maintaining these systems.

In addition to adequately sealing electrical and instrumentation panels as indicated in 8.4.2 Ingress Protection, pest and rodent deterrent mechanisms should be considered on the site.

9. Conclusion

In summary, maintaining your PROFIBUS networks and keeping them in a fully functioning healthy state is of utmost importance to prevent unnecessary downtime that results in production losses. It is critical to note that there is no single tool or piece of equipment available that will tell you exactly what the problem may be on your PROFIBUS network.

Personnel competence, knowledge, and experience (which is why certified PROFIBUS training of personnel is important), in combination with the numerous troubleshooting tools or permanent monitoring solutions available on the market, is the only way to fully understand what is causing network faults and what can be done to correct the faults.

A multimeter is not a PROFIBUS DP troubleshooting tool as this cannot be used to analyse the high-frequency switching waveforms, instead, a dedicated tool, specifically designed for troubleshooting PROFIBUS networks, must be available and relevant personnel responsible for maintaining the networks must be fully trained on how to use these tools.

Like most things, a proactive approach is the best approach. Rather identify potential issues that could cause failures before they happen so that they can be corrected during the next planned shut instead of waiting for your network to fail and then acting.

Should you experience a fault on your PROFIBUS network, do not panic and start making changes without first stopping to think why you are making the changes and being clear in your mind why your plan of action is justified. Fiddling where there may not have been an issue, in vain hope, simply opens the possibility of introducing new faults that further complicate the task of addressing the original root cause.

Instead, compose yourself and use your knowledge of PROFIBUS and the available tools, analyse the network and make calculated decisions to correct any identified issues.

10. Additional considerations – adherence to standards

PROFIBUS standards and norms define the terms, rules, and test methods for PROFIBUS networks. The below standards specify digital data communications for measurement and the interconnection of automation and process control system components by Fieldbus network systems.

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

IDX Industrial Data Xchange
The Industrial Data Communications Experts