WHITE PAPER

The process of troubleshooting a PROFIBUS DP network

Insight on typical PROFIBUS network faults and how to identify and correct these faults

What you will learn:

The best tools to use • PROFIBUS specifications and standards • Identifying common faults and fixing them • Improving network reliability and availability • Recommended training

IDX Industrial Data Xchange
The Industrial Data Communications Experts

Table of Contents

1 Introduction

1.1 Purpose of this document

The purpose of this document is to provide readers with 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 of 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. There are many scenarios that 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.

1.2 About the authors

As internationally Certified PROFIBUS Engineers and Certified PROFIBUS Trainers, employed at Industrial Data Xchange, (an internationally Certified PROFIBUS/PROFINET Competence Centre), the authors (Kyle Roos - *left* and Sean Ogborne - *right*), have accumulated many years of experience, and have a passion to empower local expertise and help our factories using PROFIBUS to maximise network availability and uptime.

They are involved in fieldbus training, fieldbus design, advanced troubleshooting, auditing, and commissioning support within the Sub-Saharan Africa region.

1.3 Industrial Data Xchange

Based in Johannesburg, South Africa, Industrial Data Xchange (Pty) Ltd or IDX, is an industrial IT company that specialises in industrial communications systems. On a day-to-day basis, IDX offers training and services related to industrial communications network health to various industries.

We have attended hundreds of PROFIBUS network audits and call outs, and as such have developed a sound fault-finding strategy and procedure.

1.4 PROCENTEC

Some of the diagnostic/troubleshooting tools discussed within this document are designed and manufactured by PROCENTEC. PROCENTEC specialises in diagnostics and analysis tools for industrial communications systems (PROFIBUS, PROFINET, and a variety of other industrial Ethernet-based protocols).

2 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:

2.1 PROCENTEC ProfiCore and ProfiTrace software

Otherwise referred to as the PROFIBUS troubleshooting toolkit, this essential piece of equipment allows you to connect into 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 health.

2.2 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 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.

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.

2.3 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.

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.

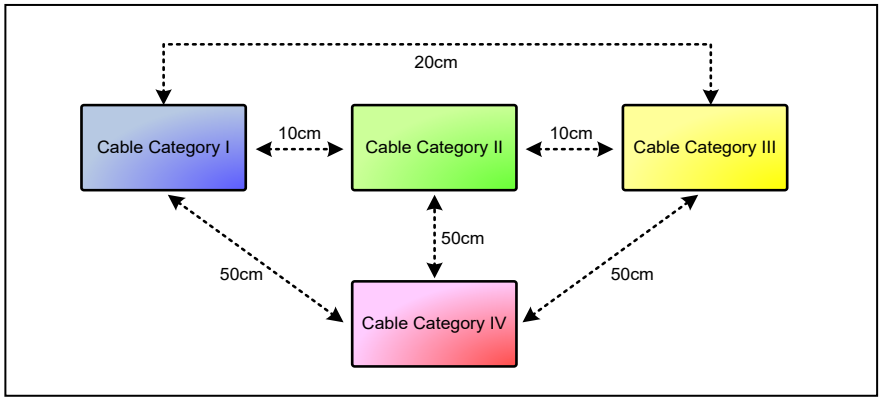
2.5 AC clamp meter

It is very useful to be able to measure the current that is traveling on the PROFIBUS cable shield. The excessive current traveling 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

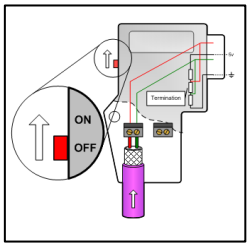
PROFIBUS cable is sensitive to inference from high voltage cables even though certain measures (shielding, differential signals, etc.) are taken to try and mitigate these effects. As a standard, the following cable distances should be adhered to for the various categories of cable:



Category I: Fieldbus and LAN cables (E.g. PROFIBUS, ASi, 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.
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).

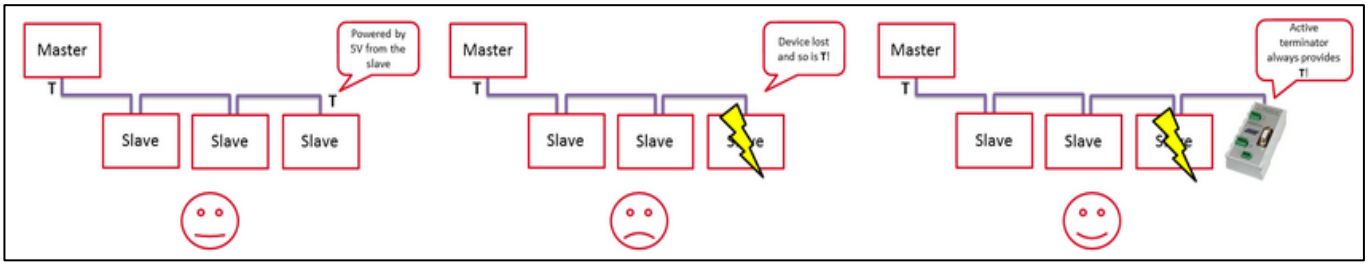
3.2 Terminations

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.



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 which requires 5V. A termination on a

connector that is enabled, but not powered (by the device it is connected to) is not terminating.

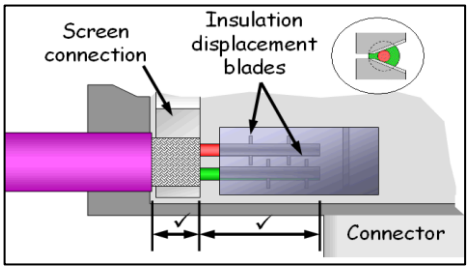


Additional note: Wherever a single wire enters a connector, the cable should always be wired into the 'incoming' port and not the outgoing, as the outgoing port is usually disconnected once the termination switch is enabled.

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" 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 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.

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 specifications and provide for 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 conductor.
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 can be utilised between any two devices on the same segment.

Baud rate	Maximum 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

3.6 Number of devices

PROFIBUS and other RS485 systems are limited to a maximum of 32 devices 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).

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 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 device should be assigned to a unique address on the network (1-125), no two devices must share the same address. Addresses are either configured through proprietary software, physical switches on the devices, or over the PROFIBUS network.

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 a termination within a network and in what cases it should / should not be enabled.

Firstly, you should always have only two terminations in each segment. The terminations should always be enabled at the beginning of the segment and at the end of the segment (where the bus ends), this may also be at an OLM or at repeating devices.

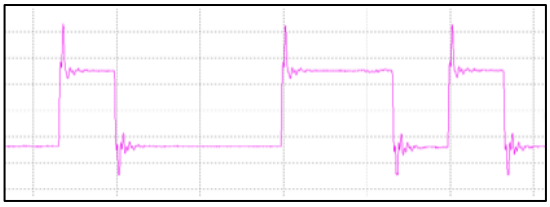
Secondly, if the termination is enabled on a PROFIBUS DP connector, the connector must always be plugged into a **powered** device as the termination circuit within the connector gets its power from the device that it is connected to.

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

4.1.1 Missing termination

As two termination 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.



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.

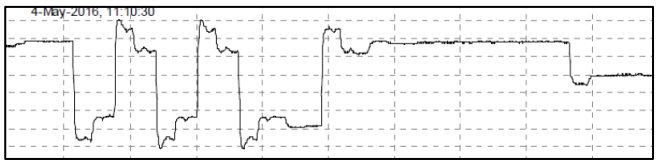
Corrective action

- 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.

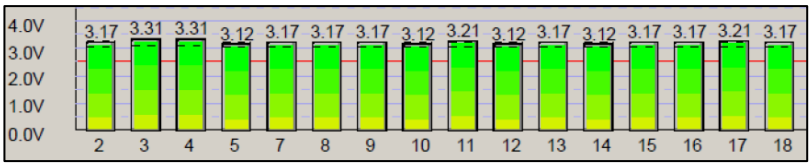
4.1.2 Over termination

An 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.



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.

Symptoms of an over termination

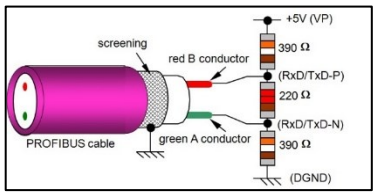
- Oscilloscope: Decreased signal amplitude and excessive ringing/reflections on the scope image.
- Voltage level: Decreased driver voltages (amplitudes of between 2 – 4 V are often detected).
- Device behaviour: Intermittent failure, loss of devices on the bus.

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.



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 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.

Both 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*.

Additionally, it is important that proper shielding and grounding mechanisms are implemented across the entire network and network environment as per section *3.4 Functional bonding and shielding*.

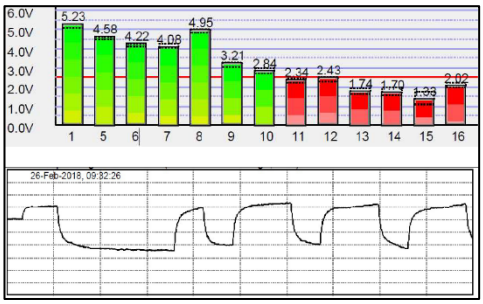
Symptoms of electrostatic/electromagnetic interference

- 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.

4.3 Long segment length



There is a limit for 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.

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.

4.4 Too many devices on a segment

The RS485 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 and 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.

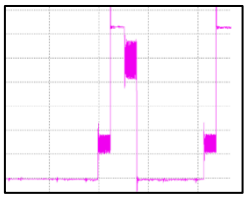
Symptoms of exceeding maximum devices per segment

- 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

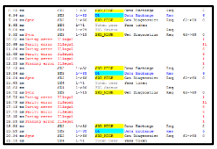
- Adjust the network topology to adhere to the maximum number of devices per segment. Consider installing repeaters and OLMs to increase the number of network segments to allow for fewer devices per segment.

4.5 Duplicate address



PROFIBUS shares a common bus (even between multiple inter-linked 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).



Duplicate addressing 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.

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 jumps up and down cyclically.
- Device behaviour: Devices at the duplicate address are intermittently lost, the entire bus may experience intermittent failure.

Corrective action

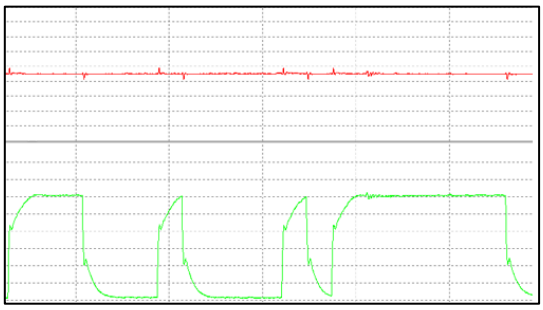
- To identify a duplicate address, unplug the suspected device to see if the fault disappears (and to see if this disconnected device's address remains on the bus). To correct a duplicate address, ensure all devices on the network have a unique address.

4.6 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).



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, 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 that was just disconnected/isolated from the bus to identify the fault.

5 Additional steps to improve network reliability and availability

5.1 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 32 PI 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 recognized certified courses:

5.1.1 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 as well as practical exercises empowers students and provides them with the knowledge to confidently maintain 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.

5.1.2 Certified PROFIBUS Engineer Course

The highest level of certification available with regards to 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 into message decoding.

How the communication between devices occurs, the successful configuration of a PROFIBUS network, 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.

5.1.3 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 call outs conducted over the years, that many PROFIBUS faults are as 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.

5.2 Permanent monitoring

A permanent monitoring solution, such as the PROCENTEC ComBricks, is a valuable 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 call outs.

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.

5.3 Network audit by a Certified PROFIBUS Engineer

Regular inspections/audits are the keys to maintaining high availability of your PROFIBUS networks, and to prevent 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 health year on 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.

5.4 Substation and RIO-panel environmental factors

5.4.1 Temperature

Although industrial electronic components, like PROFIBUS devices, mostly 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.

5.4.2 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 vertical.
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 up to 60from vertical.
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	Totally 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.

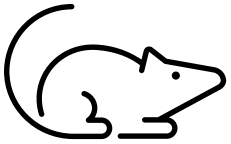
Devices installed in the field without the protection of a higher-IP rated panel should have integrated ingress protection mechanisms. Very often devices exposed to moisture and dust require, at minimum, IP65 rating within industrial environments.

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 & 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 with which the panel is installed. Do not leave any open cable ports where dust, moisture or pests can gain access.

5.4.3 Pest and rodent protection

Rodents and pests create a large risk for PROFIBUS communication networks, and can often cause damage to cabling, 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 *5.4.2 Ingress Protection*, pest and rodent deterrent mechanisms should be considered on the site.

6 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 of 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 own mind why your plan of action is justified. Fiddling where there may not have been an issue, in vain hope, simply opens up the possibility of introducing new faults that further complicate the task of addressing the original root cause. Instead, compose yourself and using your knowledge of PROFIBUS and the available tools, analyse the network and make calculated decisions to correct any identified issues.

About Industrial Data Xchange:

Industrial Data Xchange (IDX) provides industrial IT & IIoT solutions and related services to primary and manufacturing industries. We service the following sectors: food & beverage, mining & metals, power, pulp & paper, renewables, telecommunications & water, and the large EPCs & small to medium system integrators servicing these sectors. Our services include building automation, custom development, custom & legacy integration, data migration, and industrial IT consulting. IDX also provides services to help keep your control networks, especially PROFIBUS & PROFINET, running in tip-top shape. Our industrial network audits will proactively assess the health of your control networks and our industrial network emergency callouts to get you up and running when a breakdown occurs. Our developed solutions include IDX Nexus, IDX Suite, IDX Data Historian, IDX StarNet Gateway, IDX ifm VSE Gateway. We also have solutions related to building automation, IIoT, network components, network testing, and analysis tools as well as protocol converters for industrial control networks. Our IDX Academy offers internationally certified PROFIBUS & PROFINET training as well as ASi, CANbus, Modbus protocol training, and more.

Contact us for all of your connectivity challenges:
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