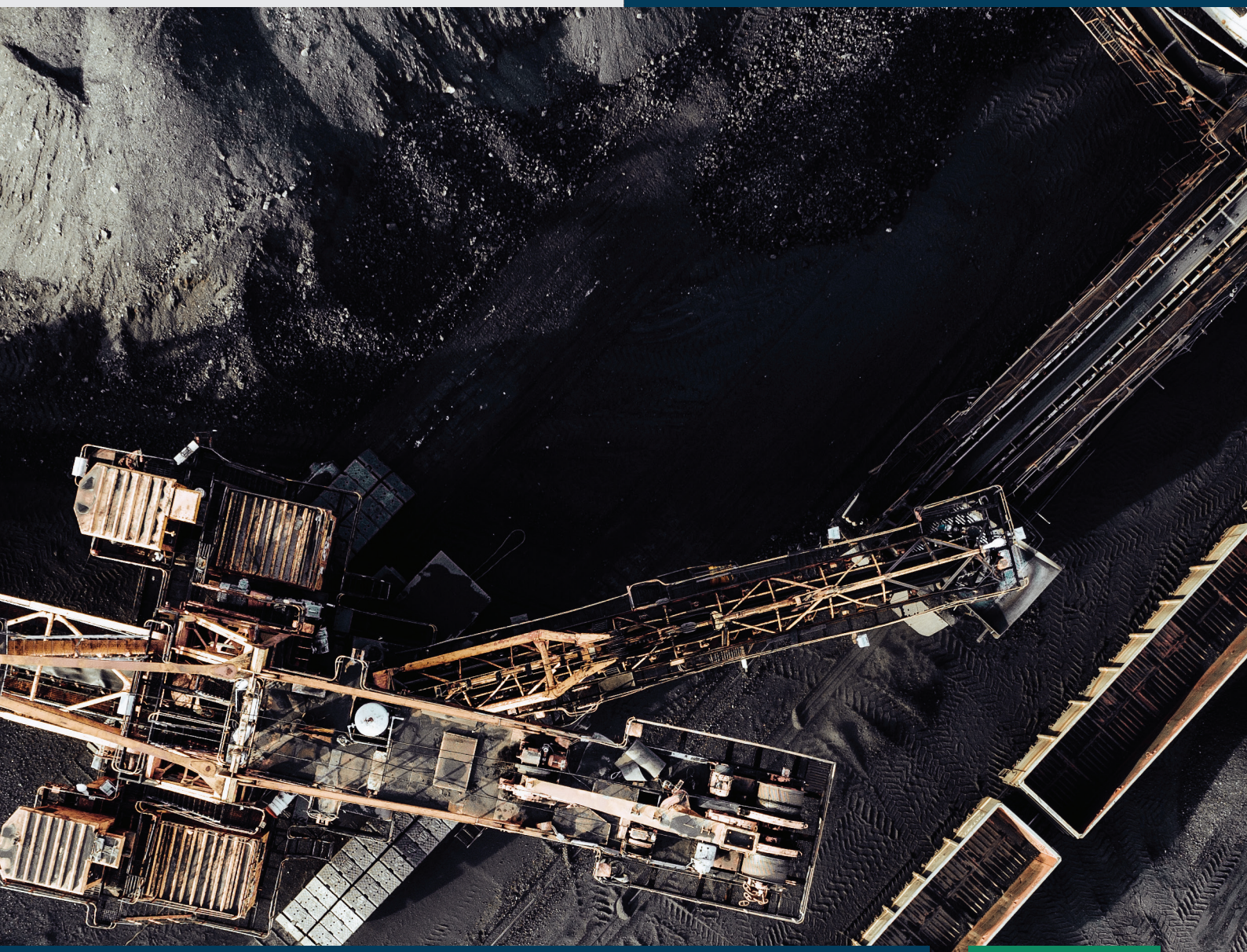
Anybus® BY HMS NETWORKS

Diagnostics



PROFINET

10 costly PROFINET mistakes you need to stop making

How network engineers can avoid the mistakes that lead to unplanned downtime and budget overspend

HMS

Introduction

PROFINET is gradually becoming the communication protocol of choice for all kinds of industries. It's already the joint biggest Ethernet-based communication protocol, and eventually, it will surpass PROFIBUS as the most popular standard network, particularly in critical applications such as process automation. As a result, having a solid understanding of PROFINET is becoming increasingly vital.

But what if your company has recently transitioned to PROFINET and you're much more familiar with PROFIBUS? Or you're fresh out of engineering school and feeling the pressure of preventing unplanned downtime?

Don't worry, we're here to help. Over the course of more than two decades, Anybus Diagnostics has encountered many field technicians unsure of the best way to set up and maintain a PROFINET network.

That's why we have developed this guide to address the most common mistakes made by PROFINET engineers. Our aim is to provide you with valuable insights and practical solutions to help you build a healthy, reliable network.

Happy reading!

Contents

MISTAKE 1:
Not stocking essential spare parts

Like any good Scout, be prepared

While PROFINET experiences fewer hardware problems than PROFIBUS, it often operates in tough environments like factories and workshops, making it susceptible to physical layer issues such as bad or broken connectors.

To ensure smooth operation, it's crucial that you maintain an inventory of essential spare parts, including:

- **Connectors**
- **Cables**
- **Grounding clips**
- **EtherMIRROR**
- **PLC cards**
- **Switches**
- **Valves**

Physical faults will occur from time to time on a PROFINET network, and you don't want to be caught unprepared.

Troubleshooting at your fingertips

You should also have a few troubleshooting tools in stock because PROFINET networks can experience as many connection problems as PROFIBUS networks.

Having a device that is dedicated to assessing the health of your industrial network and discovering any faults is a must-have tool for network engineers.

The tools of the trade

There are various troubleshooting tools that are handy to have nearby, but you should have these at least:

- **PROFINET diagnostic tool**
- **EtherTAP and a USB cable**
- **Commissioning wizard**
- **Network mapping tool**
- **Reporting device**

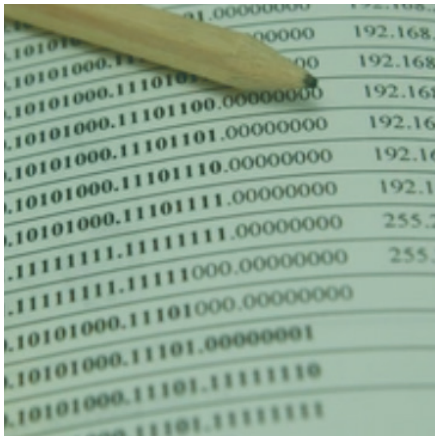
Being able to troubleshoot the moment there's a problem with your network is the best way to minimize or even prevent downtime. Couple that with having a good store of spare parts, and the cost of these essential extras will be far less than the cost of downtime.

TRUE STORY

A slaughterhouse that operates 21 hours a day, five days a week was alerted to a problem with its PROFINET network. Apparently, a valve station had failed.
A support engineer was called out and discovered a broken PLC card that needed replacing. Simple enough to fix, you'd think.

Unfortunately, the slaughterhouse didn't have a spare PLC card in stock, so it had to send one of its personnel on an emergency trip to get the part and bring it back.
The total processing downtime was eight hours at a cost of $78,000 an hour. If a spare PLC card had been in stock, it would have taken around two hours to fix the problem. That would have saved them $468,000. Ouch!

MISTAKE 2:
Not maintaining a list of occupied and available IP addresses



Eliminate double faults

Each time you add a new device to your PROFINET network, it's crucial to assign a unique, free IP address to prevent duplication.

The avoidance of duplication is vital because when multiple devices on the same network share the same IP address, conflicts occur, leading to confusion and potential network disruptions. This can keep a device offline and may even lead to the entire network shutting down.

Understand the address system

How does duplication happen? One common misconception among field technicians is that PROFINET doesn't utilize Transmission Control Protocol/ Internet Protocol (TCP/IP). As a result, they may overlook the consequences of assigning the same address to multiple communication destinations.

However, TCP/IP is indeed used in a PROFINET network when transmitting non-time-critical data, typically during configuration, parameterization, and diagnostics processes.

No more double trouble

By creating and maintaining a list of all occupied and available IP addresses for every network, you can ensure that no two devices share the same IP address. You're also making it much easier on yourself to access diagnostic information quickly and easily.

Many PROFINET networks nowadays feature embedded web servers that provide diagnostic data. To monitor your network effectively, you need to know the IP address of each device in your network.

Automate the process

Don't have a list of IP addresses, and your network is huge? Worry not. There are diagnostics platforms (like Osiris) that can do the hard work for you. They'll detect every device and every IP address on your network and create a list that you can then export for your records.

TRUE STORY

An automotive factory spent two days changing cables and connectors to no avail after discovering a fault on their PROFINET network.

Finally conceding defeat, they called in their support engineer, who plugged in a Mercury diagnostic tablet and found the issue in just one minute.

It turned out that a newly installed device had been assigned a duplicate IP address. Once the device was given a new IP address, it was up and running again.

If only the factory had kept a list of assigned IP addresses (sigh).

Atlas2 Plus


USB1
USB2
FACTORY
OFFICE
RELAY
-
+ 12-24VDC
SH
Anybus
BY HMS NETWORKS
Atlas

MISTAKE 3:
Ignoring PROFINET design, installation, and commissioning guidelines

PROFINET is not PROFIBUS

It may sound obvious, but it's worth stressing the point: PROFINET is not PROFIBUS. So, it follows that you shouldn't apply PROFIBUS rules when installing a PROFINET network.

Yet some field technicians do just that, mistakenly believing that because both protocols have a common source and the same application, they can be installed in the same way.

Serial vs. Ethernet

PROFIBUS is the classic automation protocol based on serial communication, while PROFINET is a newer protocol based on Industrial Ethernet. This key difference results in various disparities when setting up your network.

The topologies are different. So are the physical interfaces, transmission rates, cycle times, network loads, and cable lengths.

Follow the guidelines

Following PROFINET guidelines during set up ensures a robust network from the outset. You'll be able to (among other things):

- **organize your network topology in a way that best suits your devices and their functions**
- **measure and plan for real-time and non-real-time network loads**
- **install cabling and connectors correctly**
- **assign IP addresses and device names appropriately**
- **configure real-time IO devices according to their PROFINET GSD (GSDML) files**

By following the guidelines, you can ensure a successful installation right from the beginning, minimizing the risk of device issues and network failures. Read the guidelines, you (and your boss) will be pleased you did.

TRUE STORY

During the commissioning phase of a recently installed PROFINET network, a manufacturer encountered repeated network failures. However, the installers (who were much more familiar with PROFIBUS) couldn't understand why the network was failing.

Several hours later, they tracked the problem to signal loss in a cable. Puzzled, they looked up the installation guidelines and realized the cable was too long (it was 200m).

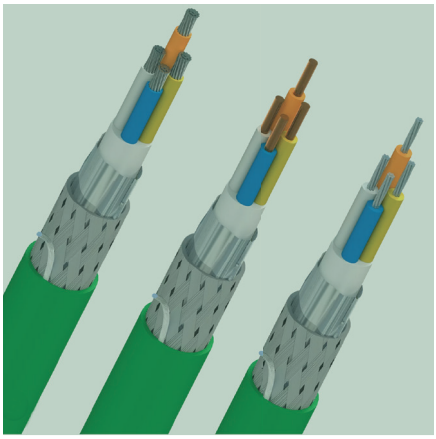
The maximum length of a cable for a PROFIBUS network depends on the baud rate. The higher the transmission speed, the shorter the cable length per segment. So, a 200 m cable is fine if the baud rate is 1.5 Mbps.

But for PROFINET, the maximum distance between two endpoints of communication when using copper cabling is only 100 m.

The installers had to take the cable out and replace it with two shorter cables and a switch, wasting a great deal of valuable time.

MISTAKE 4:

Assuming official PROFINET cables are a waste of money



Recognize a false economy

It may be tempting to use standard Ethernet cables throughout your PROFINET network. After all, they're cheaper than official PROFINET cables, and you may already have some in stock.

However, it will cost you far more in the long run. Why? Because standard Ethernet cables cannot adequately protect your network from electromagnetic interference (EMI).

More protection, less to worry about

PROFINET cables are specifically designed with shields and sheaths that protect the copper wire from EMI. They also have more twists per inch than basic cable, which helps eliminate crosstalk, and they're much more flexible, which gives them a narrower bend radius.

This flexibility is crucial for moving applications or applications with continuous flex. Repetitive motion or a permanent curve will eventually distort and break standard cables, bringing down your network.

Consider your environment

Does this mean you need PROFINET cables in all situations? Probably not. In office environments with minimal electronic stress, you can use standard Ethernet cables.

However, in harsher environments such as workshops or on the factory floor, where network stability can be compromised by factors like EMI, mechanical stress, dirt, extreme temperatures, and vibrations, PROFINET cables are essential.

DID YOU KNOW?

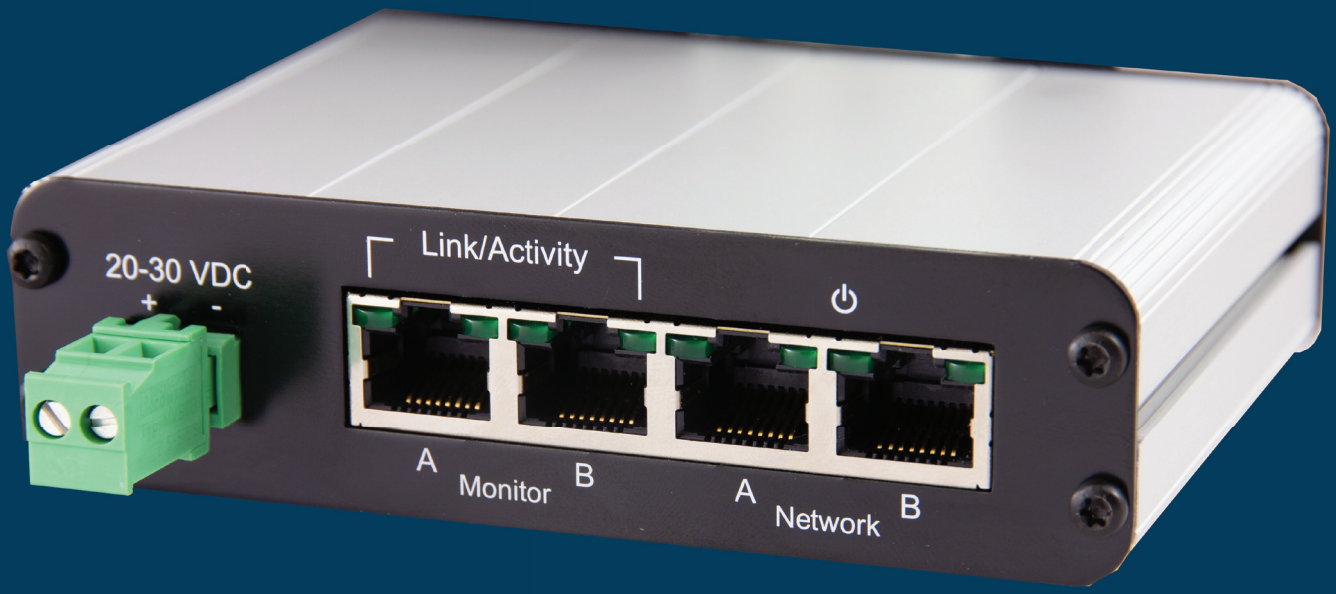
ROFINET cables, like standard Ethernet cables, ensure correct signal impedance, meaning they adjust the resistance to electrical current flow based on the signal frequency.

However, PROFINET cables are specifically designed for fixed or dynamic flexible automation applications, making them ideal for industrial Ethernet setups.

Still not convinced? Consider this analogy: Imagine buying a water-resistant jacket for regular hikes in the hills, only to find yourself drenched during a downpour.

You end up calling a taxi to take you home and dry off. The water-resistant jacket turned out to be a false economy. Instead, investing in a more expensive, purpose-built waterproof jacket would have been the wiser choice.

EtherMIRROR



MISTAKE 5:

Bundling power cables with PROFINET cables

Gross interference

Power cables can disrupt the performance of data cables if they're bundled together. Since the magnetic field of the current running through a power cable is much bigger in comparison, it can easily interfere with the signals of a data cable.

Looping the cables or tying them up tightly only makes matters worse.

A policy of segregation

To protect your PROFINET cables from picking up disturbances from power cables, you need to keep them separated. The standard distance of segregation for unshielded power cables with a voltage of 220 volts or higher is 20 cm.

However, you can reduce that distance by using a bridge, tray, or rack. These come in a range of different materials but note that they don't all offer the same level of protection.

Steel vs. aluminium

For example, an aluminum shield in a closed conduit reduces radiation between your 220-volt power cables and PROFINET cables, so you only need a 10 cm separation.

A steel shield provides even better protection against radiation, allowing for a separation of only 5 cm.

TRUE STORY

During the commissioning phase of a PROFINET network in a waste-to-energy power plant, an engineer noticed the absence of segregation between power cables and data cables.

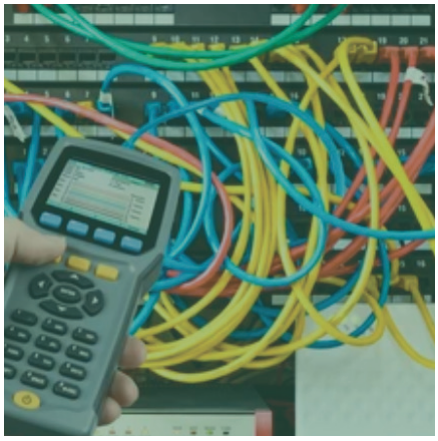
He realized that the resulting EMI would be so severe that it would bring the entire network crashing down.

He ordered steel bridges to be installed for the entire cabling system, and the commissioning phase was able to continue.

Crisis averted. And time, as we all know, is money.

MISTAKE 6:

Downplaying the importance of certifying PROFINET cables



Healthy cables, healthy network

Cables are the nervous system of any PROFINET network. Even if your network is well-designed and properly installed, using sub-standard cables and connectors will inevitably lead to disruptions and eventual network failure.

That's why it is essential to not only perform cable testing but also prioritize cable certification, especially during the commissioning phase.

Spot your problems sooner, not later

Certifying your cables requires the use of a cable certifier, as a standard cable tester won't suffice. While a tester can verify correct wiring and connections, it cannot detect potential cabling issues such as:

- **incorrect lengths**
- **rogue devices**
- **misconfigured nodes**
- **return loss**
- **crosstalk**
- **insufficient impedance and attenuation**

The highest standards where it matters

Unlike testers, cable certifiers meet the stringent cabling standards of ISO and TIA (the best ones can even test network traffic). That means they can verify that your cables meet all regulatory specifications such as bandwidth and frequency. They even let you add the characteristics of any custom cabling you may have.

Fortunately, there's usually no need to certify every single cable in your network. Focus on your primary PROFINET cables.

Since these cables are permanent installations and difficult to replace without shutting down the network, they're the ones that will lead to unplanned stoppages.

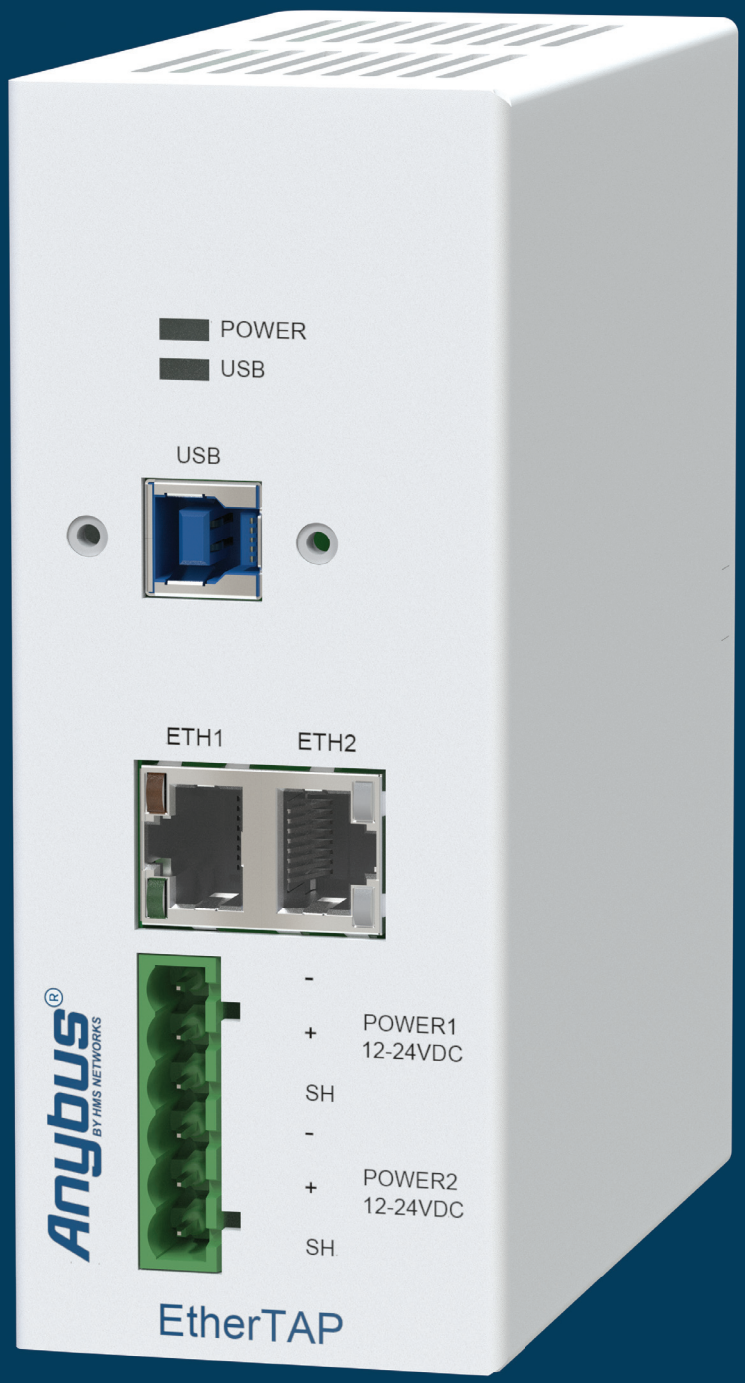
DID YOU KNOW?

Across all industries, the average cost per hour of downtime is $260,0001. While cable certifiers don't come cheap (around €10k), they can save you thousands in the long run by preventing downtime, not to mention the cost of new cabling and wasted labor hours.

This is particularly true when installing a new network, as damaged, broken, or incorrectly installed cables are a common cause of downtime for new PROFINET sites.

1The Aberdeen 2016 Report: Maintaining Virtual System Uptime in Today's Transforming IT Infrastructure, 2016.

EtherTAP2


POWER
USB
USB
ETH1
ETH2
-
+
POWER1
12-24VDC
SH
-
+
POWER2
12-24VDC
SH
Anybus
BY HMS NETWORKS
EtherTAP

MISTAKE 7:
Using a switch's monitor port to do passive monitoring

The importance of passive monitoring

Active monitoring has been mentioned a few times in this guide, and rightly so because it's super important for giving you a real-time view of your network's performance.

However, when you're troubleshooting, passive monitoring can be a useful supplement to active monitoring. In fact, if you have a critical network, 24/7 passive monitoring is an absolute must.

Spot those dropped packets

Unlike active monitoring, passive monitoring provides actual user data over a specific period, making it highly effective in detecting dropped packets—small units of data that fail to reach their destination.

Packet loss can occur for various reasons, such as a poor connection or network congestion.

Tapping into your network

The best way to passively listen to network messages is to use an EtherTAP (Traffic Access Point).

This is a hardware device with two ports that allows you to access and monitor your data without interfering with your network or losing any messages.

The limitations of monitor ports

So why not use the monitor port of a managed switch to do passive monitoring? Because the monitor port relies on the switch's capabilities.

If the switch can't handle a high network load when dealing with real-time data, it can affect the monitor port and compromise the data you're analysing. Packets will be dropped, and port mirroring will stop working (or work intermittently).

The ultimate solution

Unlike a monitor port, an EtherTAP is a passive device that sends and receives data streams simultaneously, eliminating the risk of dropped packets. It also captures everything on the wire, even when the network is saturated.

DID YOU KNOW?

Experienced trouble-shooters tend to look at the passive monitoring results first. They find it extremely useful to see actual network issues before making any changes based on active monitoring (which is basically predictive data).

Passive monitoring covers more performance data and a much wider range of metrics compared to active monitoring, so it provides a lot of useful analytics. Not only dropped packets but also cycle times, alarms and jitters.

Not sure where to install a TAP? The best place is between the PLC and the first switch. That placement gives you a real measure of what is going on in your network because all data has to pass through these two points.

MISTAKE 8:
Not having any free network ports

A sub-optimal scenario

Imagine having a kitchen with only three electrical sockets: one for your fridge-freezer, one for your oven, and one for your dishwasher. Whenever you want to use your microwave, toaster, or washing machine, you have to unplug one of those three other appliances.

The problem is that you always forget which cable runs to your fridge-freezer, so you cross your fingers and hope you don't pull out the wrong plug and disconnect it by mistake. Not optimal, right?

Don't force yourself to choose

The same principle applies to your PROFINET network. Whenever you want to do some active monitoring or conduct an audit, you don't want to have to unplug something from your network just to connect a diagnostics tool.

That's especially true if you're unsure which cable to unplug because you don't know which device it's connected to. At best, you risk disconnecting a device; at worst, you risk an unplanned stoppage.

Always have one or two free ports

Ensure you always have at least one port available for diagnostic and measuring purposes. Two is even better. Then, if you have a problem with one port, you have a backup.

TRUE STORY

What was supposed to be a simple one-day audit turned into an expensive two-night affair.

Unfortunately, the engineer couldn't proceed with the audit as planned due to the absence of free ports.

The only opportunity to connect the diagnostic tools to the network was during the site's daily maintenance period, which was between 3 am and 5 am.

As a result, the company had to pay for an extra day's audit plus expenses.

MISTAKE 9:
Using unmanaged switches throughout your network

Have a backup in the event of failure

Unmanaged network switches are cheap, easy to use, and connect a device instantaneously, so why aren't they the ideal option for your PROFINET network? Because they don't allow you to monitor, manage and configure your network's settings. Unmanaged network switches simply pass on data exchange messages through the correct port. That basic functionality is fine for small, non-critical networks with a fixed configuration and one or two switches.

However, for networks where downtime is not an option, such as a power plant, you need to build some redundancy into your network.

Managed vs. unmanaged switches

If you have a failure somewhere in your network, you don't want it to bring down the entire system.

Let's say you have a faulty device and you don't know to which port it is connected. An unmanaged switch won't alert you, it won't tell you which port the device is connected to, and it won't be able to do anything about the error. It will just stop working.

A managed switch, on the other hand, is intelligent enough to find another path to the message's destination. This ensures network availability and decreases the risk of a data communications failure. It also decreases your troubleshooting time considerably.

More flexibility, more security

Managed switches really are the backbone of your network because they enable you to understand and diagnose the health of your network. They let you:

- **adjust each port to any setting you desire, enabling you to monitor and configure your network in many ways**
- **prioritize channels**
- **duplicate data to another port**
- **customize security**
- **use SNMP to relay network configuration data to offsite network engineers, reducing troubleshooting time and increasing uptime**

There are various brands and types of switches on the market, ranging from low-end to high-end. The best are dedicated PROFINET managed switches because they contain a mini-PROFINET device, which gives you all the diagnostic data you need.

DID YOU KNOW?

Manufacturers of managed switches often disable SNMP (Simple Network Management Protocol) at the point of sale. Therefore, you will likely need to manually enable it yourself.

MISTAKE 10:
Not having an Ethernet mirror available in every network

Maximizing the efficiency of your TAP

Using an EtherTAP to monitor a network is the most reliable way to capture live performance data. However, when it's time to audit or maintain your PROFINET network, you don't want to break your connections or shut down your network just to install an EtherTAP.

What's more, if you have several non-critical networks, you don't really want to install an EtherTAP on every network. That could be expensive.

Easy access with Ethernet Mirrors

The low-cost, least-problematic option to both these situations is to mount an EtherMIRROR on every network. These passive Industrial Ethernet Measuring Points give your EtherTAP easy access to your network, avoiding interruptions to your data communications and eliminating the need for downtime.

And, unlike mirror ports, EtherMIRRORs don't overburden a switch's CPU or drop packets on heavily used networks.

Making diagnostics a walk in the park

Because Ethernet mirrors are passive devices, there's nothing else to do once you've installed them. They just sit there allowing data to go through them. When you need to access your passive monitoring data, simply connect an EtherTAP to an EtherMIRROR and perform your diagnostics.

TRUE STORY

When it was time to do a network audit for a logistics company, the visiting engineer needed a free port to connect the EtherTAP between the PLC and the switch.

Unfortunately, the company was confused about which ports were routed to which devices. The wrong cable was removed, which led to the accidental shutdown of the entire plant.

The company quickly learned the importance of knowing the topology of your PROFINET network, keeping a free port for audit and maintenance work, and installing an EtherMIRROR on every network.

Introducing Anybus Diagnostics

Anybus Diagnostics is a leading provider of diagnostic and monitoring solutions for the industrial automation market. They specialize in developing and manufacturing high-quality automation products for PROFIBUS, PROFINET, Industrial Ethernet, EtherNet/IP, and EtherCAT networks. Their products, including ProfiTrace, ProfiHub, ComBricks, Osiris, Mercury, and EtherTAP, are highly recognized and used by customers worldwide.

To ensure engineers are equipped with the skills needed to design, install, maintain, and troubleshoot industrial networks effectively, Anybus Diagnostics offers a certified PROFIBUS and PROFINET Competence and Training Centre. The Anybus Diagnostics Academy has already certified over 4,000 engineers to implement and maintain their PROFINET and PROFIBUS networks to the highest standards available.

Work with HMS Networks.
The number one choice for
industrial communication
and IIoT.

Anybus® BY HMS NETWORKS Ewon® BY HMS NETWORKS Intesis® BY HMS NETWORKS Ixxat® BY HMS NETWORKS

HMS Networks - Contact

HMS is represented alll over the world. Find your nearest contact here:

www.hms-networks.com/contact

HMS

www.hms-networks.com