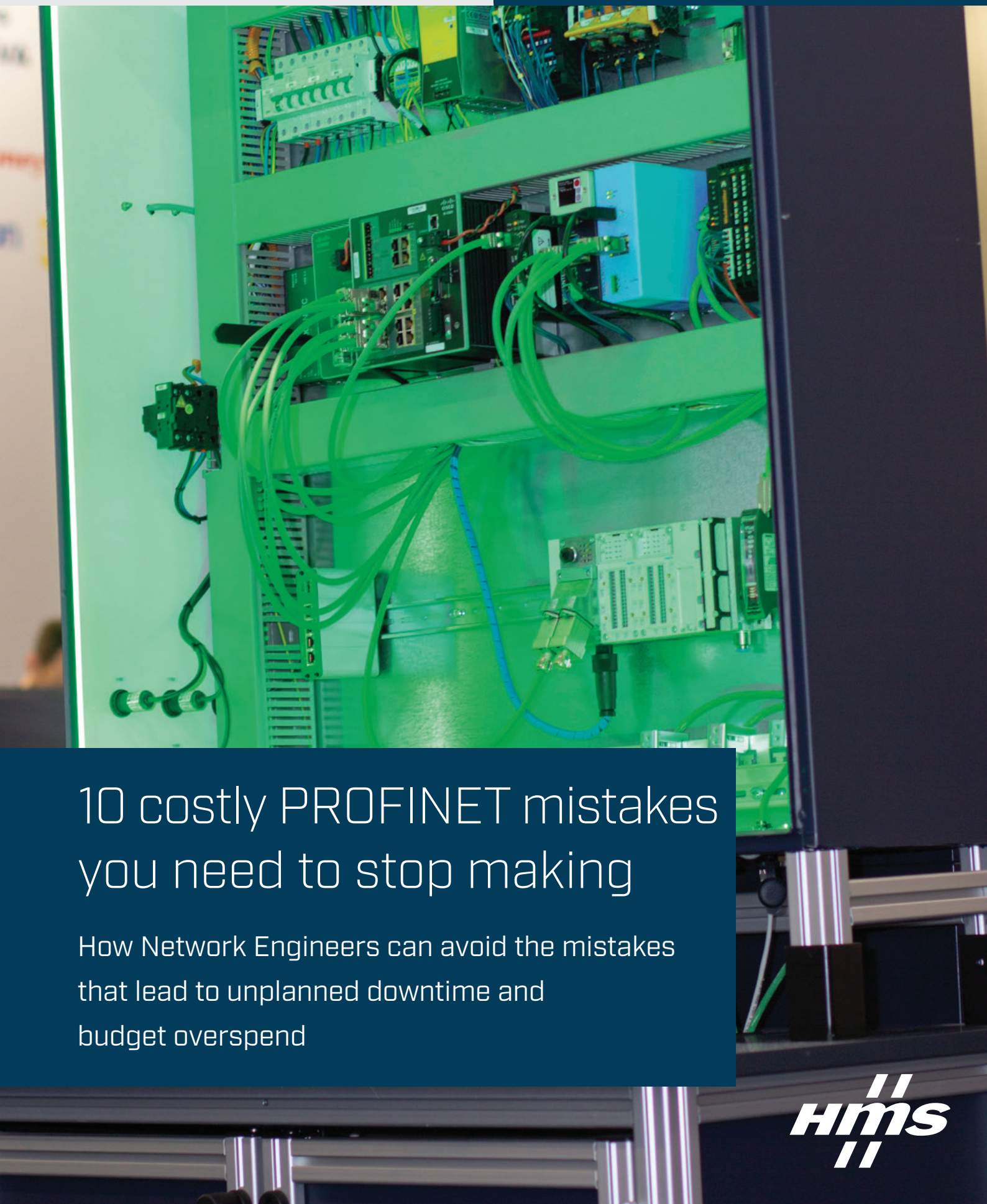
Anybus® BY HMS NETWORKS

Diagnostics



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. Eventually, it will surpass PROFIBUS as the most popular standard network, particularly in critical applications. In fact, it's already joint market-leader alongside EtherNet/IP among the various versions of Ethernet-based communication solution for industrial automation. 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 stress of preventing unplanned downtime?

We can assure you that you're not alone.

In our more than twenty years of experience at Anybus Diagnostics, we've come across many field technicians unsure of the best way to set up and maintain a PROFINET network. And that is why Anybus Diagnostics has decided to produce this guide to the most common mistakes made by PROFINET engineers.

We hope that you find it incredibly useful and that it will help you provide a healthy, reliable network.

Contents

MISTAKE 1:
Not stocking essential spare parts

Like any good Scout, be prepared

PROFINET doesn't suffer quite as many hardware problems as PROFIBUS. However, it does often operate in dirty environments like factories and workshops, so it can have physical layer problems like bad or broken connectors.

Therefore, make sure you have a good stock of essential spare parts such as:

- **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**

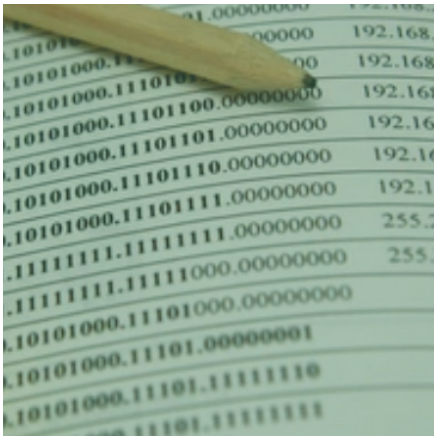
Being able to troubleshoot the moment there's a problem with your network is the best way to minimize or even prevent downtime. Couple that with having a good store of spare parts, and the cost of these essential extras will be far less than the cost of downtime.

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

Every time you add a new device to your PROFINET network, you need to assign a free IP address. This avoids duplication.

Avoiding duplication is important. When two or more devices on the same network are given the same IP address, conflicts arise and your network becomes confused. This can keep a device offline and may even lead to the entire network shutting down.

Understand the address system

How does duplication occur? One reason is that many field technicians wrongly believe that PROFINET doesn't actually use Transmission Control Protocol/Internet Protocol (TCP/IP). Consequently, they overlook the implications of two communication destinations being assigned the same address.

However, TCP/IP is used in a PROFINET network when the data being communicated is not time critical. This is typically during configuration, parameterization and diagnostics.

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.

These days, many PROFINET networks have embedded web servers that provide diagnostic information. So, if you want to see what is happening on your network 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 platform (like Osiris) that can do it for you at the click of a button. 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

Know your protocols

It's an obvious thing to say, 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, in the mistaken belief 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, whereas PROFINET is a newer protocol based on Industrial Ethernet.

This gives rise to several 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**

Avoid device issues and network failures by making a good job of the physical installation the first time round. You (and your boss) will be so glad you did.

TRUE STORY

A manufacturer was going through the commissioning phase of its recently installed PROFINET network. 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).

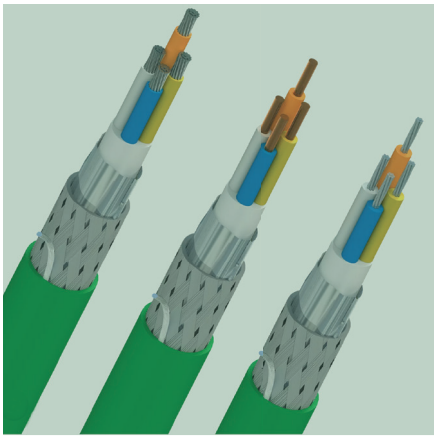
The maximum length of a cable for a PROFIBUS network depends on the baud rate. The higher the transmission speed, the shorter the cable length per segment. So, a 200 m cable is fine if the baud rate is 1.5 Mbps.

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



Know a false economy when you see it

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 end up costing 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 have 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.

That last point is particularly relevant for moving applications or applications that have a continuous flex. Repetitive motion or a permanent curve will eventually distort and break standard cables, and that will bring down your network.

Consider your environment

Does this mean you need PROFINET cables in all situations? Probably not. For example, you could use standard Ethernet cables in an office environment. That's because it's not as stressful for electronic communication.

In areas like the workshops and the factory floor, the stability of your network can be adversely affected by EMI, mechanical stress, dirt, extreme temperatures and vibrations. In harsher environments, PROFINET cables are much more suitable.

DID YOU KNOW?

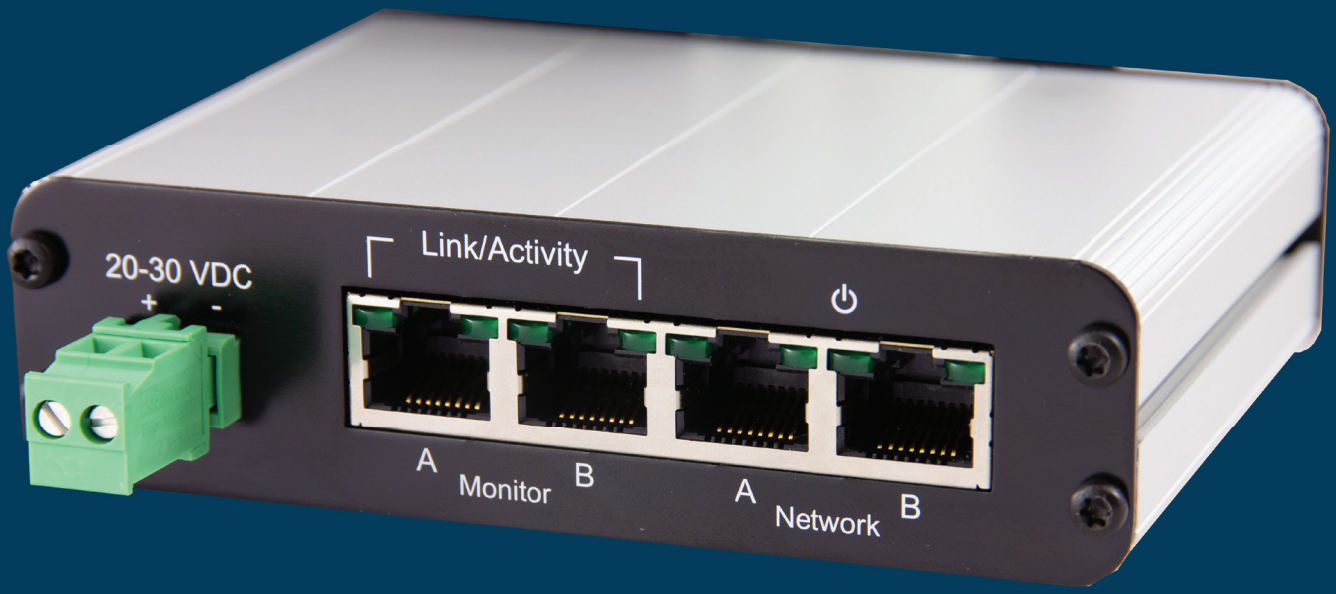
Like standard Ethernet cables, PROFINET cables guarantee to transmit signals at the correct impedance. In other words, they ensure that the amount of a component's resistance to the flow of electrical current will vary according to the signal's frequency.

However, PROFINET cables are much more suitable than standard cables for fixed or dynamic flexible automation applications. Basically, they are industrial Ethernet cables.

Not convinced? Think of it like this. You decide to buy a water-resistant jacket to go hiking regularly in the hills. Then you get caught in a downpour and realize you are soaked through.

You end up calling a taxi to pick you up and take you home to dry out. The water-resistant jacket was a false economy. You should have bought that more expensive, fit-for-purpose waterproof jacket.

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 that are 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 aluminium shield in a closed conduit reduces radiation between your power cables and PROFINET cables to a level that requires only a 10 cm separation.

However, a steel shield provides even better protection against radiation, so you need a separation of only 5 cm.

TRUE STORY

A power plant that converts waste to energy was about to enter the commissioning phase of its PROFINET network.

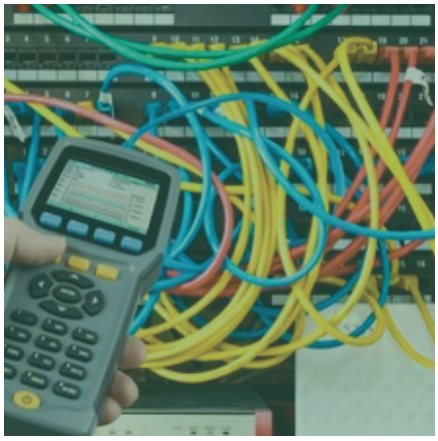
While checks were being made, a visiting engineer spotted the lack of segregation between the power cables and the data cables.

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, costs money.

MISTAKE 6:

Downplaying the importance of certifying PROFINET cables



Healthy cables, healthy network

Cables are the nervous system of any PROFINET network. No matter how well designed or installed your network is, if your cables and their connectors are sub-standard, nothing else will work properly and your network will go down.

And that's why you need to do more than test your cables. You need to certify them as well, especially during the commissioning phase.

Spot your problems sooner, not later

To certify your cables, you need to use a cable certifier. A standard cable tester can't do the job. Yes, a tester verifies that your cables are wired correctly. But it's only testing your connections. What a tester can't do is identify 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.

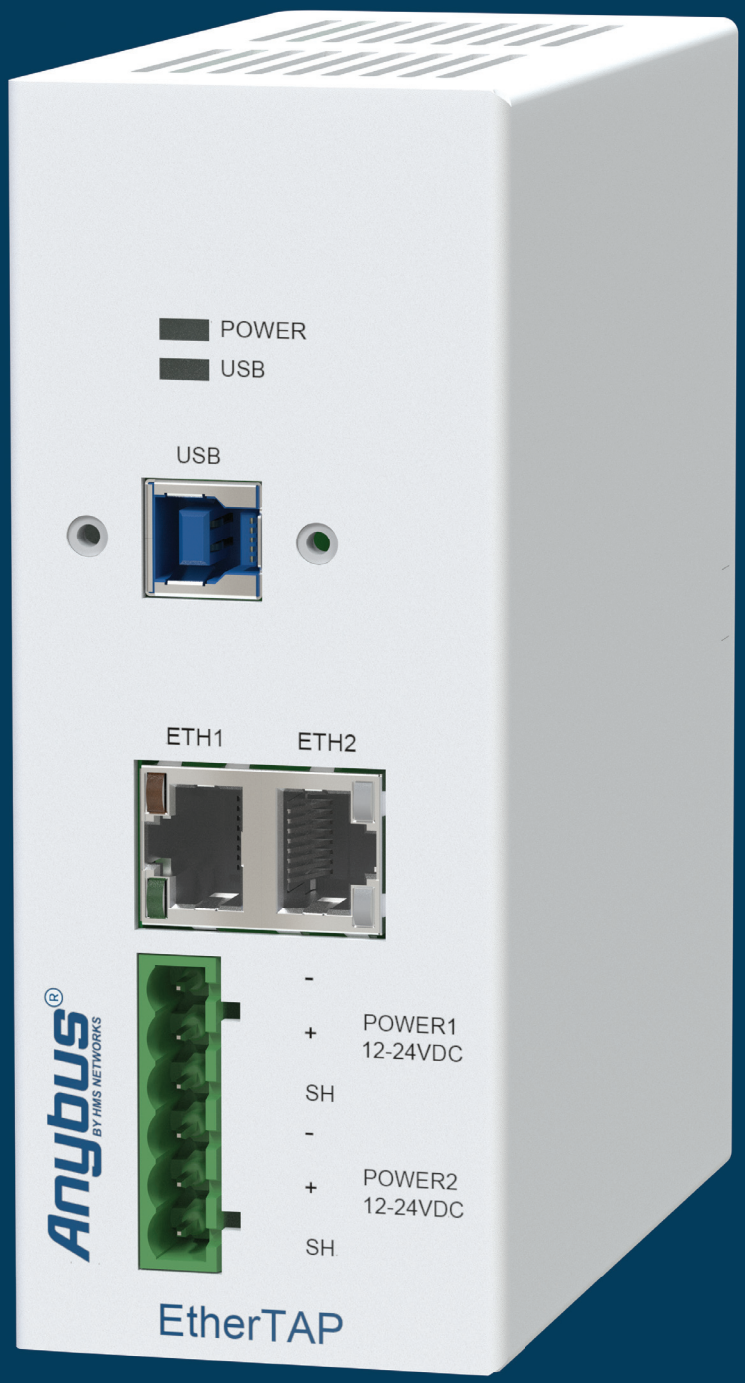
DID YOU KNOW?

Across all businesses, the average cost per hour of downtime is $260,000 (The Aberdeen 2016 Report: Maintaining Virtual System Uptime in Today's Transforming IT Infrastructure, 2016).

Cable certifiers don't come cheap (around €10k), but they can save you thousands in the long run by avoiding your company costly downtime, not to mention the cost of new cabling and wasted labour hours.

This is especially true if you're installing a new network. Damaged, broken or incorrectly installed cables are a common cause of downtime for new PROFINET sites.

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 gives you actual user data over a specific period. This makes it really effective at discovering dropped packets (i.e. a small unit of data that fails to reach its destination).

Packet loss can happen for a number of reasons, for example a bad connection or network congestion.

Tapping into your network

The best way to listen passively to all the messages being passed around your network is to plug in an EtherTAP ("TAP" is an acronym for "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, so there's no 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 first.

Trouble is, 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

It's pretty much the same with 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

Make sure 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 back-up.

TRUE STORY

An external network engineer was called out to conduct a PROFINET audit at a large logistics company. It should have been a simple one-day audit. It turned out to be an expensive two-night audit.

Unluckily, the engineer couldn't do the audit as planned because there were no free ports. The only time it was possible to connect the diagnostic tools to the network was during the site's daily maintenance period. And that was between 3 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 back-up 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 only 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 (like a power plant), you're going to want 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. So, you'll probably have to physically 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 can work out 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.

But, when the time comes to access your passive monitoring data, you simply plug an EtherTAP into an EtherMIRROR and run 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 plug in the TAP 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 lead to the accidental shut down 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.

Are you a PROFINET technician wanting to upskill?

Anybus Diagnostics makes it easy for you to develop your PROFINET skills and increase your confidence. It provides a range of training opportunities for all needs and budgets, from three-hour online tutoring to in-depth certification courses.

You'll get:

- Access to experts with years of experience in the field
- Digestible online learning bites with clear instructions (Bytesize Training)
- Internationally recognized certificates of training (for certified courses)
- Technical theory combined with practical exercises
- High quality training customized for any industry

If you work every day with PROFINET, or if you supervise those that do, you'll find these professional courses an excellent investment. You'll know how to implement and make use of a widely used automation technology. More importantly, you can ensure your company won't have to face unexpected, costly downtime due to avoidable mistakes.

Discover our courses

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