The convergence of OT and IT from a Diagnostics Point of View

Contents

Chapter 1

Introduction to Diagnostics in Operational Technology

Operational Technology (OT) deals with all the technology used to control a factory or process plant. In the last 30 years, it has seen three significant changes. The first was the introduction of proprietary serial-based communications protocols. The second was the introduction of Open serial-based communications protocol. The third has been the more recent introduction of Information Technology into their world.

Open communication protocols are protocols that no one company owns and are 'open' to every company to implement. Before the rise of open protocols, OT had only proprietary protocols, protocols owned by one company, and available only to them.

Information Technology (IT) deals with all the technology used by a business for daily operations centred around the office environment. Today, we have many open protocols that make use of Ethernet standards that come from IT. This so-called convergence of OT to IT has created many challenges and opportunities.

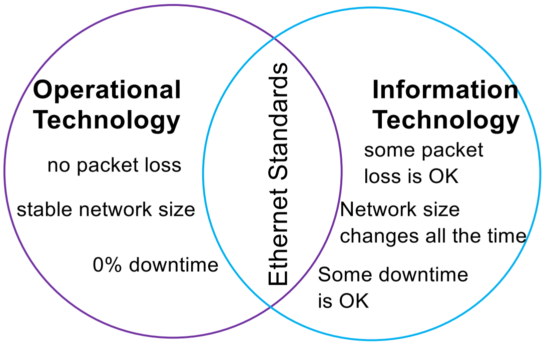


Figure 1: The convergence of OT and IT – they share Ethernet standards but have different goals and priorities

The change from proprietary to open protocols and the introduction of IT has had a massive effect on how people maintain and troubleshoot their systems, including what diagnostics are available and how they are handled. This paper will examine how this has developed over time and how it has addressed or not addressed end-users needs.

Basic needs of OT

Factories and process plants need to run continuously for years with as few interruptions or maintenance as possible. The dream of any plant manager is to commission a plant, where they only had to throw one switch, and the process would start and continue to work on its own for the next 30 years – no downtime and no maintenance.

It is a great goal, but it is a fantasy. In the real world, things break down, and we must fix them. It is possible through good design and installation methods to minimize maintenance. Unfortunately, even for these perfectly designed and installed plants, devices still age and fail; the mechanical proximity switch can only flip so many times before needing replacement. The robot cable is designed to move a lot, but even flexible cable can only be bend so many times. The screw that you tightened down will, through temperature changes and vibration, eventually loosen.

Maintenance is a necessary evil. It is necessary because we must do it. If we do not, the factory or process plant will simply stop working! It is evil because it is not something that a business wants to spend money on.

For maintenance to be effective, the plant technician must know what is going on and where to fix things. They get this information by using diagnostics. There are three diagnostic class types: process diagnostics, device diagnostics, and network diagnostics.

Process diagnostics are things like the vessel temperature is too hot, packages are all clumped up on the belt, or low flow. Process diagnostics are sorted out by the design engineer when the plant or factory is designed.

Device diagnostics are things like the input is shorted out, or the output card is not responding, or the sensor malfunctioned. Device diagnostics are typically incorporated into the communication protocol.

Network diagnostics are things like a device that has dropped off the network or a lost packet. Network diagnostics are partially incorporated into the communication protocol itself and partially external.

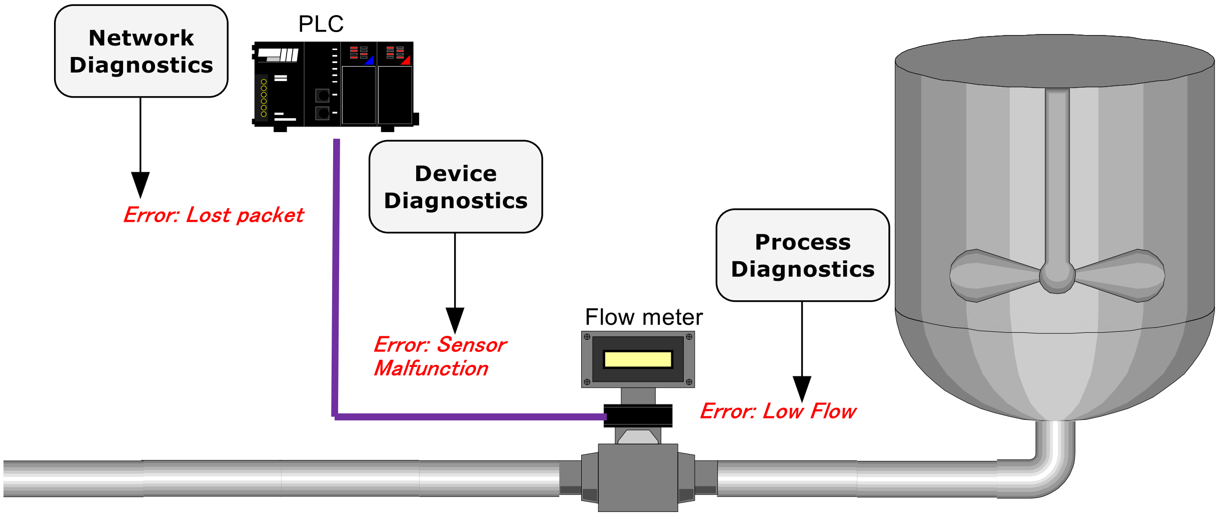


Figure 2: The three classes of diagnostics: Network, Device, and Process

Since Process diagnostics are the realm of the process design engineers, we will focus on device and network diagnostics.

Proprietary Protocols

When industrial networks were first introduced, they were all proprietary. Vendors had mixed feeling about these types of protocols. They tended to like the fact that once their protocol was picked, the plant or factory had to buy all of their devices from the vendor. However, if the plant or factory did not select their protocol, then they would lose sales. Also, the vendors had to maintain the protocols.

End-users liked the cost savings from implementing distributed networks but did not like being closely tied to one vendor.

Most of the proprietary protocols that I worked with did an excellent job with device diagnostics and a lousy job with network diagnostics.

Network diagnostics presented quite a problem for the vendors. Since they owned the protocol, they did not want to share information about the protocol with anyone. If they did, then another company could 'steal' this information and build a better protocol that could be used against them. The result was that troubleshooting these networks was complicated even for the vendor's field-service engineers. End-users had extraordinarily little information about the protocol and few, if any, network diagnostics. Most of the time, the most you had, was some sort of live list of who was on the network.

The cost of this was huge when you think of the cost of downtime. Proper network diagnostics will significantly reduce the time it takes to get the network back online. Without these diagnostics, end-users are stuck spending time going over each node, hoping that they would stumble on the problem.

Open Protocols

The first open protocols were all serial protocols. PROFIBUS, DeviceNet, ControlNet, Modbus, to name a few.

Some of these open protocols, PROFIBUS, for example, built-in a method for handling Device diagnostics just like some of the proprietary protocols did.

This time, however, information about the protocols were available to the end-user. This led to the development of excellent user-friendly network diagnostic tools. ProfiTrace is a prime example of this sort of tool. With troubleshooting tools like ProfiTrace, end-users could not only significantly reduce downtime, they could also prevent them. They prevented downtime, by checking on the health of the network before it went down and then doing preventive maintenance to prevent unscheduled downtime.

Figure 3: The author troubleshooting PROFIBUS using Osiris running on Mercury with a Proficore

Also, the protocol itself included some network diagnostics. These diagnostics would be recorded in the controllers. Unfortunately, all of the controllers I have worked with did not do a very good job processing and displaying this information. In many sites, both Device and Network diagnostics were shown to the end-user as one error labelled 'Channel' error.

Ethernet-based Protocols

Ethernet-based protocols are protocols that use the Ethernet physical layer and make use of other protocols that use this physical medium. They have typically been based on the evolution of their serial predecessors. PROFIBUS formed the basis to develop PROFINET. DeviceNet and ControlNet formed the basis to build EtherNet/IP. Modbus TCP is based on Modbus RTU.

These Ethernet-based protocols all have the perception of having higher bandwidth and functionality while offering lower costs and more versatile wiring than their serial predecessors. These perceived benefits can be argued. However, their easy tie-in to higher systems and the enormous possibilities of standard Ethernet can not be argued. By all measurements, Ethernet protocols are taking over.

In the case of PROFINET, the protocol designers learned from their PROFIBUS experience and made the handling of both Device and Network diagnostics even better. Also, this new design made it such that the control vendors were pretty much forced to display these diagnostics correctly – no more confusion over device and network diagnostics.

Summary of Chapter 1

In moving from proprietary to open serial and then to open Ethernet-based protocols, we have seen a continuous improvement in how diagnostics are handled. In the next chapter, we will focus on network diagnostics and see what the actual requirements are. We will then go back to the examples of PROFIBUS and PROFINET and see what is happening with those protocols.

Chapter 2

OT Network Diagnostic Requirements

When an OT network specialist looks at any industrial network, they want to know:

- Who is on the network?
- Has anyone joined or dropped off the network?
- Any packet losses?
- What are the update times and jitter?
- What is the network loading?
- Any diagnostic messages?

The number of devices on the network should be constant in most applications. In the odd application, there may be backup devices that are only used for over-load conditions or when maintenance is required on one of the primary devices – these applications are the exception. Therefore, seeing who is on the network and being able to tell who has dropped off or joined the network is very valuable.

Control systems need to have constant update times in order to handle data on time. You can imagine if the command to open a push bar arrives after the product has already gone past – you are no-longer controlling the flow of that product. As a result, they need a deterministic network with no packet losses. A packet loss causes a delay, and this is bad. Most systems are designed so that one packet loss is not a big deal. However, control systems assume that a packet loss is an exception, not the rule.

When you design a control system to maintain control, your system requires a minimum update time. Knowing what your update times are and that they match what you want is essential. Jitter is the variation in cycle times, and minimizing this variation is important for control.

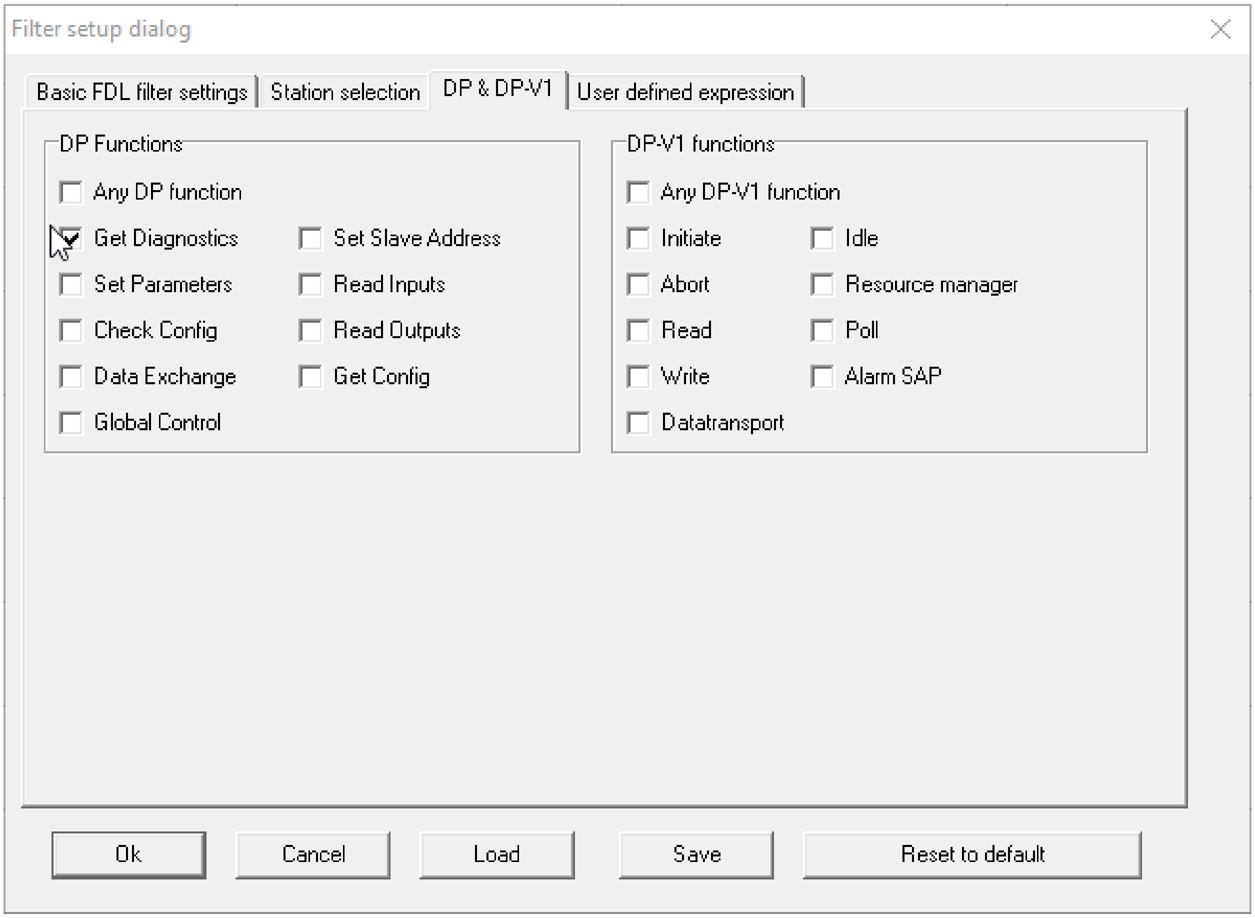
Network loading is related to update times and is dependent on the type of network you have. Most serial protocols are designed so that as you increase the network load, your update times go up linearly. In Ethernet-based protocols, network load has little to no effect on update times until it hits a certain level where switches start to get overloaded and then it has a significant effect on the network. See it as a traffic jam: busy roads are no problem, but too many vehicles will overload the intersection.

Diagnostic messages are either generated because of a process fault, device fault or network issue. In normal operations, you want none of these to occur.

PROFIBUS Experience:

Looking at the list of OT network diagnostic requirements, I can easily remember the early days of PROFIBUS and how hard it was to find out any of that information. These were the days of the Amprolyzer (Advanced Multicard PROfibus AnaLYZER) bus monitor. This software was not only not user-friendly, it was downright user-hostile. For example, if you wanted to know if there were any diagnostic requests happening on the network, you had to know that you had to filter on a Destination Service Access Port (DSAP) of 3C. In other words, if you did not know the protocol down to the hexadecimal level, you could not use this tool.

Flash forward to today. We have PROFIBUS bus monitors like ProfiTrace, where this information is a click away.



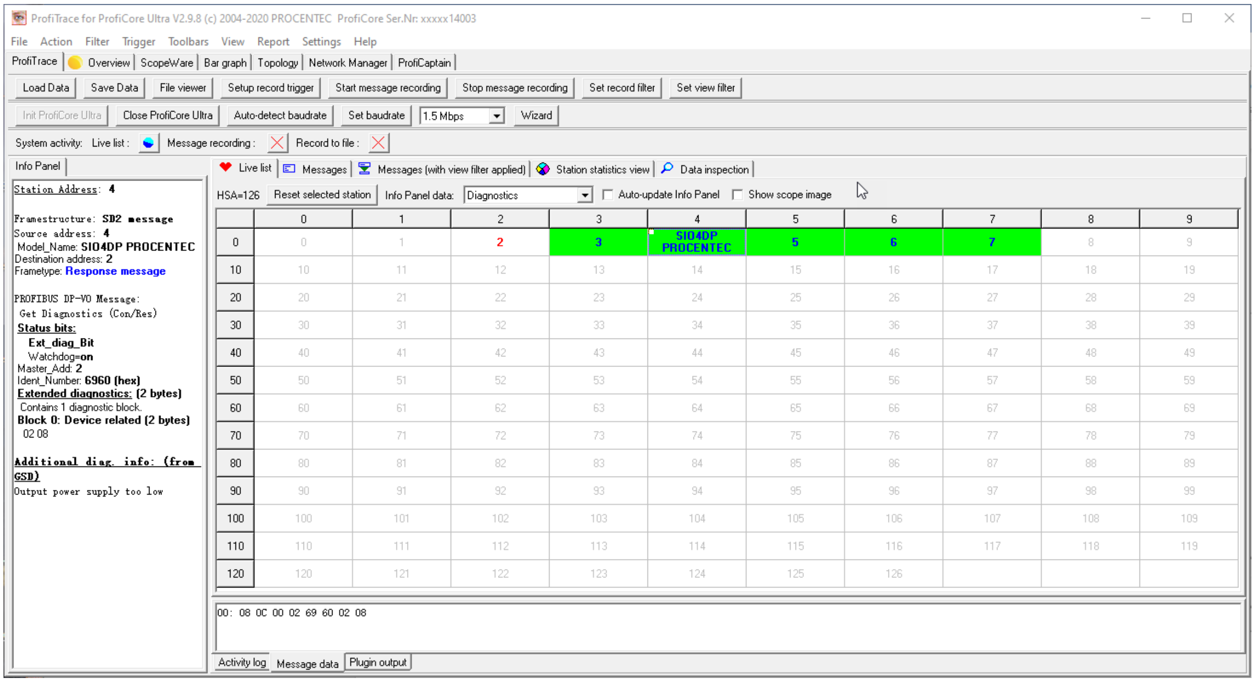
DP Functions

- ☐ Any DP function
- ☑ Get Diagnostics
- ☐ Set Slave Address
- ☐ Set Parameters
- ☐ Read Inputs
- ☐ Check Config
- ☐ Read Outputs
- ☐ Data Exchange
- ☐ Get Config
- ☐ Global Control

DP-V1 functions

- ☐ Any DP-V1 function
- ☐ Initiate
- ☐ Idle
- ☐ Abort
- ☐ Resource manager
- ☐ Read
- ☐ Poll
- ☐ Write
- ☐ Alarm SAP
- ☐ Datatransport

Figure 4: With ProfiTrace, to filter on Diagnostic messages, it is a simple check box



Set baudrate: 1.5 Mbps

HSA=126

Info Panel data: Diagnostics

☐ Auto-update Info Panel

☐ Show scope image

Station Address: 4

Framestructure: SD2 message
Source address: 4
Model_Name: SIO4DP PROCENTEC
Destination address: 2
Frametype: Response message

PROFIBUS DP-V0 Message:
Get Diagnostics (Con/Res)
Status bits:
Ext_diag_Bit
Watchdog=on
Master_Add: 2
Ident_Number: 6960 (hex)
Extended diagnostics: (2 bytes)
Contains 1 diagnostic block.
Block 0: Device related (2 bytes)
02 08

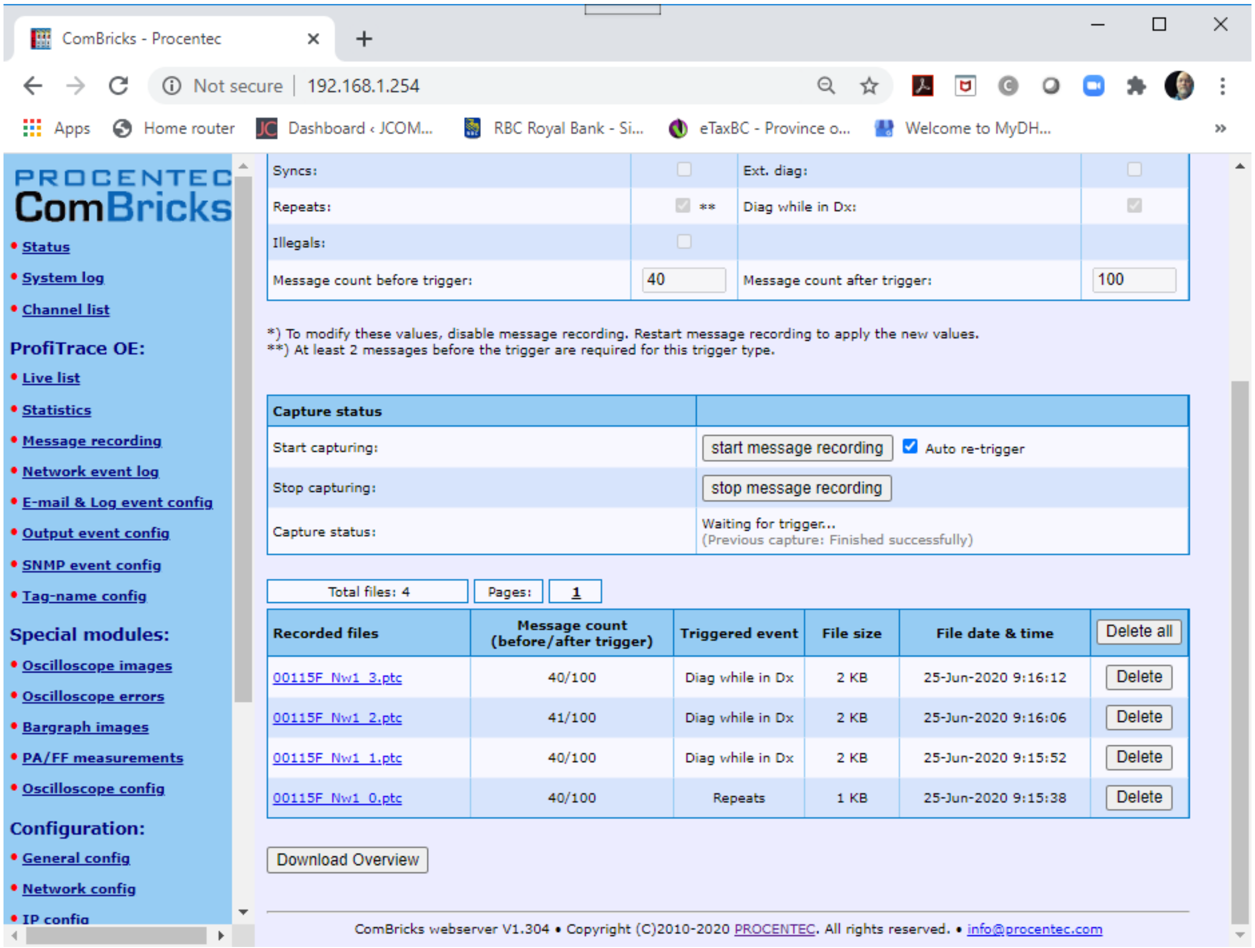
Additional diag. info: (from GSD)
Output power supply too low

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	SIO4DP PROCENTEC	5	6	7	8	9
10	10	11	12	13	14	15	16	17	18	19
20	20	21	22	23	24	25	26	27	28	29
30	30	31	32	33	34	35	36	37	38	39
40	40	41	42	43	44	45	46	47	48	49
50	50	51	52	53	54	55	56	57	58	59
60	60	61	62	63	64	65	66	67	68	69
70	70	71	72	73	74	75	76	77	78	79
80	80	81	82	83	84	85	86	87	88	89
90	90	91	92	93	94	95	96	97	98	99
100	100	101	102	103	104	105	106	107	108	109
110	110	111	112	113	114	115	116	117	118	119
120	120	121	122	123	124	125	126			

```
00:  08  0C  00  02  69  60  02  08
```

Figure 5: In ProfiTrace, the decoded diagnostic message is displayed in the Live List

ProfiTrace is almost the perfect OT troubleshooting tool. The only problem was that it could not look back in history and see what happened on the network before you plugged it in. You had to wait for the problem to occur again. That is why PROCENTEC developed COMBRICKS, a permanent monitoring system with built-in ProfiTrace. This product is a maintenance person's dream come true. It sits on your network 24 hours a day, seven days a week, every day of the year and records what is going on. When you get a call that the operator thinks that something is wrong, you can quickly log on and see everything you need to know. Who is on the network? Has anyone dropped off? When did they drop off? What was the diagnostic message? Was the diagnostic message caused by a device issue or a network issue?



Syncs:	□	Ext. diag:	□
Repeats:	☑ **	Diag while in Dx:	☑
Illegals:	□		
Message count before trigger:	40	Message count after trigger:	100

*) To modify these values, disable message recording. Restart message recording to apply the new values.
**) At least 2 messages before the trigger are required for this trigger type.

Capture status	
Start capturing:	start message recording ☑ Auto re-trigger
Stop capturing:	stop message recording
Capture status:	Waiting for trigger... (Previous capture: Finished successfully)

Total files: 4 | Pages: 1

Recorded files	Message count (before/after trigger)	Triggered event	File size	File date & time	Delete all
00115F_Nw1_3.ptc	40/100	Diag while in Dx	2 KB	25-Jun-2020 9:16:12	Delete
00115F_Nw1_2.ptc	41/100	Diag while in Dx	2 KB	25-Jun-2020 9:16:06	Delete
00115F_Nw1_1.ptc	40/100	Diag while in Dx	2 KB	25-Jun-2020 9:15:52	Delete
00115F_Nw1_0.ptc	40/100	Repeats	1 KB	25-Jun-2020 9:15:38	Delete

Download Overview

ComBricks webserver V1.304 • Copyright (C)2010-2020 PROCENTEC. All rights reserved. • info@procentec.com

Figure 6: COMBRICKS showing the history of what happened on the network and when!

Industrial Ethernet Experience

In many ways, I would say that we are still in the early days of Industrial Ethernet. Protocols like PROFINET, EtherNet/IP and Modbus TCP have been around for a while and are being used all over the place. However, many are small projects. More extensive networks are only now becoming more common.

One interesting fact that we have discovered about industrial Ethernet is that it is tough to mess up a small installation. I have seen several that have been thrown together and not designed, yet they worked fine. The problems and need for network diagnostics only came about as they started to expand their network.

When I first started working with Industrial Ethernet, the main tool for troubleshooting was Wireshark. This is a well-known tool for troubleshooting Ethernet, and although it is not 'user hostile' like Amprolyzer, it shares the requirement that the user needs to know a fair bit about the protocol they are trying to troubleshoot. Wireshark is a great tool that I will keep in my tool kit but does suffer from presenting you with way too much information. So much so that the old British expression of not being able to see the forest for the trees is very true with Wireshark.

With Wireshark, you could, in theory, find almost any problem on the network. However, this is going to take even a Wireshark expert a lot of time. Therefore, there is a definite need for a ProfiTrace/COMBRICK type product for Industrial Ethernet. Luckily, these products exist. In Chapter 4, we will summarize the monitors currently available.

Chapter 2 Summary

In this chapter, we have gone over the requirements of OT. In the next chapter, we will focus on IT-OT convergence, what are IT requirements and how OT and IT are different.

Chapter 3

IT – OT Convergence

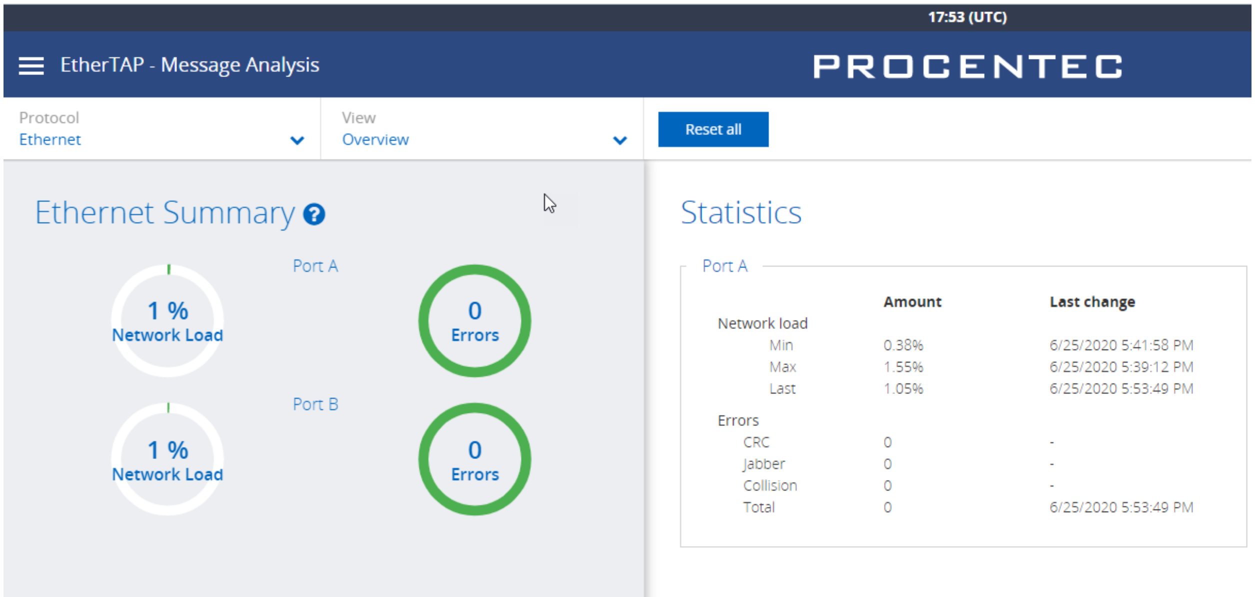
As soon as OT started using Ethernet, IT started getting involved. Many IT departments believe that anything with an Ethernet port belongs to them. As we will show in this chapter, getting IT involved is a good thing. Having them as owners may not be the best option.

Diagnostics from IT

IT has developed many software tools to help them manage an Ethernet network. Protocols such as Simple Network Management Protocol (SNMP), Internet Control Message Protocol (ICMP), and Link Layer Discovery Protocol (LLDP), to name a few. Excellent tools that OT is now making use of. However, just as an axe can be used by both a lumberjack and an artist, how they use it, and the result is vastly different.

Let us look at two of these protocols, SNMP and ICMP, to see how they are used differently. SNMP is used to pull a wealth of information from all nodes on a network. The data is stored in the Management Information Base (MIB's). IT will use SNMP to see who is on the network, the overall topology, and key performance indicators. OT is also interested in who is on the network and what is the overall topology. However, OT expects the topology to be precisely the way they designed it – no changes from day-to-day. IT will see the topology as fluid, changing by the hour. When looking at who is on the network, OT will be checking to see that all the same model of devices will have the same firmware version. This is because two devices that are the same model but with different firmware could cause issues on the network. IT may look at firmware versions, but not with the same importance as OT.

ICMP has the famous 'ping' command in it. Ping is very useful to see if other nodes are 'visible' from the one you are on. It is a great troubleshooting tool that every IT manager uses. OT managers will use it too, but for two reasons. First, is the same one as IT, to verify that one node is visible from another node. This command can also be used as a pro-active method of determining if there are line issues or switch problems. Remember, OT wants to have no lost packets while IT is fine with having some. For example, if an IT person sees that twice a day one of the switches has a 2% packet loss they might want to see if they could off-load any traffic around those peak periods, but it would not be a big deal. However, an OT person will be genuinely concerned about that event and want to investigate what is happening.



Protocol: Ethernet

View: Overview

Port A

1 % Network Load

0 Errors

Port B

1 % Network Load

0 Errors

Port A

	Amount	Last change
Network load		
Min	0.38%	6/25/2020 5:41:58 PM
Max	1.55%	6/25/2020 5:39:12 PM
Last	1.05%	6/25/2020 5:53:49 PM
Errors		
CRC	0	-
Jabber	0	-
Collision	0	-
Total	0	6/25/2020 5:53:49 PM

Figure 7: Osiris showing measured Netload going into the PLC complete with Error monitoring.

Requirements of IT vs OT

The requirements of OT compared to IT are vastly different:

- IT deals with varying data sizes that can be huge, while OT data tends to be very small in comparison.
- Packet delay is important for IT, but not like it is for OT. A one second delay in IT is not a problem. In OT, a 100ms delay can mean disaster.
- In many cases, IT people can come to the office in the middle of the night to work on the network or even briefly interrupt the network at lunch with no issues. OT situation is completely different. OT's networks typically run 24 hours a day, seven days a week, every week of the year with no interruptions at all. Most of the time, these plants will have a short window of scheduled downtime a couple of times a year to do maintenance.
- OT requires the deterministic behaviour of data packets. The data needs to arrive on time, all the time, with no lost packets. Otherwise, the control does not work correctly. In the early days

of IT, Ethernet had packets collide. The network was known as a Carrier-Sense Multiple Access / Collision Detection (CSMA/CD). The messages all eventually got through after the collisions, but sometimes there were delays. Switches have eliminated collisions, but the protocols that IT uses, such as TCP/IP, still have mechanisms for re-transmission. As a result, IT has the mindset that delays are OK and that the odd lost packet is no big deal. OT has the opposite mindset – everything on time and no lost packets.

- The number of devices on an OT network is either fixed or varies a little bit. For example, 30 devices with four backup drives that only join the network when needed. However, in IT, the number of users varies considerably. The management of users is one of the critical functions of IT.
- OT devices must have fixed addresses, while IT devices use a pool of addresses. Again, this comes down to the fixed versus varying natures of the two worlds.
- IT focuses on both Local area networks and Wide area networks and connects the Internet. On the other hand, OT is focused primarily on the control network, which in most cases is a local area network.
- IT has had to deal with network security for a long time. OT, not so much. For most of the time that OT has existed, any network that they used was so specialized and removed from the public that they were secure by default – how can you hack what you can not get to or see. With the Ethernet-based industrial protocols, this situation has changed. Security is perhaps the most significant opportunity for IT to help OT.
- Updates are handled differently. Since IT has been so concerned with Security in a Wide area network world, rolling out security patches as they come out has become very common in IT. On the other hand, OT likes to get a network/system working perfectly and then make no changes. A software update is viewed as a potential source of bugs that might disrupt the factory/plant. Therefore, any software update must be rolled out very carefully in OT.

Chapter 3 Summary:

In this chapter, we learned that IT and OT have different perspectives on how a network operates and, therefore, have different network diagnostics requirements. Next, we will look at what tools are available for both IT and OT.

Chapter 4

Ethernet Troubleshooting tools

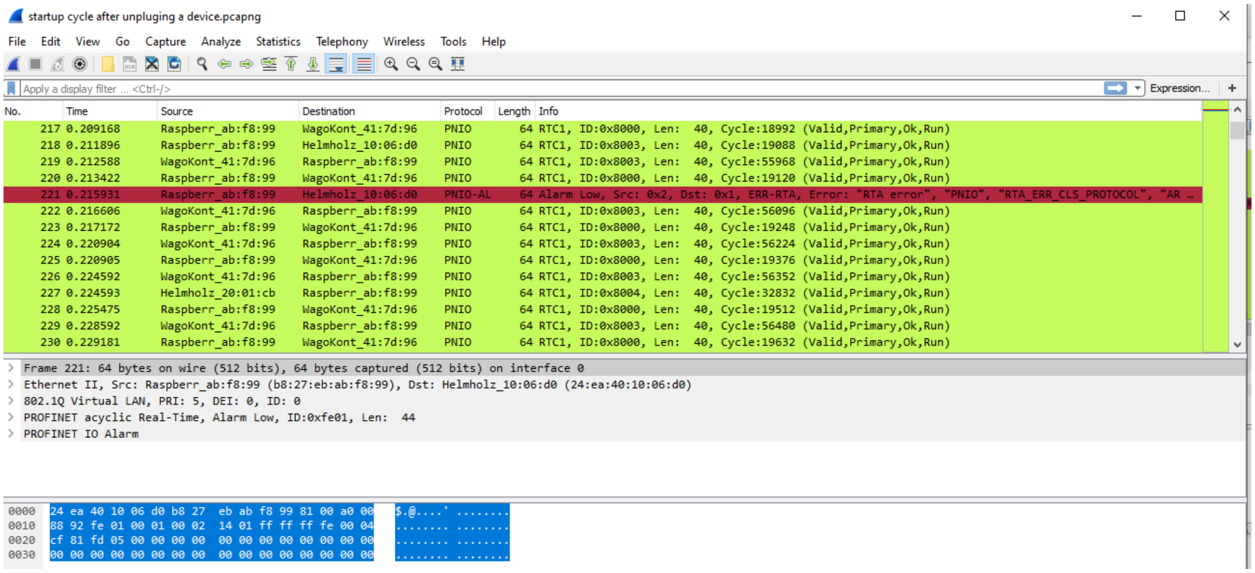
This chapter will be a quick overview of the monitor tools currently available on the market. To make it easier, we will divide the monitors into three categories: packet sniffers, IT tools, and OT tools. All of these monitors use either passive, active or both methods for collecting data.

A passive monitor sits on the network and monitors packets. They derive all of their information from looking at packets and do not send out any messages. They contribute nothing to the Netload of the network.

An active monitor will sit on the network and use different Ethernet protocols to gather information about the network. The two most popular Ethernet protocols for this function are SNMP (Simple Network Management Protocol) and ICMP (Internet Control Message Protocol). Monitors designed for PROFINET will also use DCP (Discovery and basic Configuration Protocol) and PROFINET acyclic commands to get Identification and Maintenance (I&M) Functions information. These monitors will contribute to the Netload of the network. However, if they are designed and set up correctly, their load will have a minimum impact.

Packet Sniffers

Although there are a couple on the market, Wireshark is by far the most popular. This is a tool that gives you a view of your network traffic at the packet level. This is a strictly passive monitor. As I have mentioned before, this tool presents far too much information for most people and problems. This is a tool for a network specialist and would only be used occasionally.


startup cycle after unpluging a device.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source              Destination         Protocol  Length Info
  217 0.209168  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:18992 (Valid,Primary,Ok,Run)
  218 0.211896  Raspberr_ab:f8:99   Helmholz_10:06:d0   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:19088 (Valid,Primary,Ok,Run)
  219 0.212588  WagoKont_41:7d:96   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:55968 (Valid,Primary,Ok,Run)
  220 0.213422  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:19120 (Valid,Primary,Ok,Run)
  221 0.215931  Raspberr_ab:f8:99   Helmholz_10:06:d0   PNIO-AL       64 Alarm Low, Src: 0x2, Dst: 0x1, ERR-RTA, Error: "RTA error", "PNIO", "RTA_ERR_CLS_PROTOCOL", "AR …
  222 0.216606  WagoKont_41:7d:96   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:56096 (Valid,Primary,Ok,Run)
  223 0.217172  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:19248 (Valid,Primary,Ok,Run)
  224 0.220904  WagoKont_41:7d:96   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:56224 (Valid,Primary,Ok,Run)
  225 0.220905  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:19376 (Valid,Primary,Ok,Run)
  226 0.224592  WagoKont_41:7d:96   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:56352 (Valid,Primary,Ok,Run)
  227 0.224593  Helmholz_20:01:cb   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8004, Len:  40, Cycle:32832 (Valid,Primary,Ok,Run)
  228 0.225475  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:19512 (Valid,Primary,Ok,Run)
  229 0.228592  WagoKont_41:7d:96   Raspberr_ab:f8:99   PNIO          64 RTC1, ID:0x8003, Len:  40, Cycle:56480 (Valid,Primary,Ok,Run)
  230 0.229181  Raspberr_ab:f8:99   WagoKont_41:7d:96   PNIO          64 RTC1, ID:0x8000, Len:  40, Cycle:19632 (Valid,Primary,Ok,Run)
```

```
> Frame 221: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
> Ethernet II, Src: Raspberr_ab:f8:99 (b8:27:eb:ab:f8:99), Dst: Helmholz_10:06:d0 (24:ea:40:10:06:d0)
> 802.1Q Virtual LAN, PRI: 5, DEI: 0, ID: 0
> PROFINET acyclic Real-Time, Alarm Low, ID:0xfe01, Len:  44
> PROFINET IO Alarm
```

```
0000  24 ea 40 10 06 d0 b8 27  eb ab f8 99 81 00 a0 00   $.@....' ........
0010  88 92 fe 01 00 01 00 02  14 01 ff ff ff fe 00 04   ........ ........
0020  cf 81 fd 05 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Figure 8: Wireshark PROFINET capture

IT Tools

IT has many vendors providing tools to help them manage their networks. For example, here is a small list: SolarWinds Network Performance Monitor, Site24x7, Atera, Nagios Core, Pandora NMS. These are great tools, but they were all written with IT and their requirements in mind. As we already saw in Chapter 3, OT and IT have vastly different perspectives. These tools will use many of the same protocols that OT tools will, but they will not highlight the same issues.

Also, these tools are limited to using the standard Ethernet protocols such as SNMP and ICMP. They will not use either DCP or Acyclic PROFINET communications.

OT Tools

Operations Technology also has fewer vendors than IT since it is a smaller market. The major ones are Softing, CSMT, Hilscher, Indu-Sol and PROCENTEC.

The Softing product, TH Link, is good as one would expect from Softing. This is a strictly active monitor. It provides basic information about the network:

- a live list with SNMP information on each node
- firmware check to verify the same type of devices are all at the same firmware level
- Detection of configuration errors
- Detection of device failure

TH Link uses a software package called TH Scope that must be loaded onto a computer and will get and display information from several TH Links. This topology has its pluses and minus. It is nice to be able to gather information on multiple networks into one program. However, everyone who wants to view this information must have a license for this software and install it on their computer. Also, this product has not seen many updates. The released notes, posted online, was last updated in 2017.

CSMT Polo Tecnologico in Italy is a PROFINET competence center that has developed a PROFINET network test program called PNT Pro. It is the only tool listed here that only does PROFINET. The rest of them will also do EtherNet/IP and other Ethernet-based protocols.

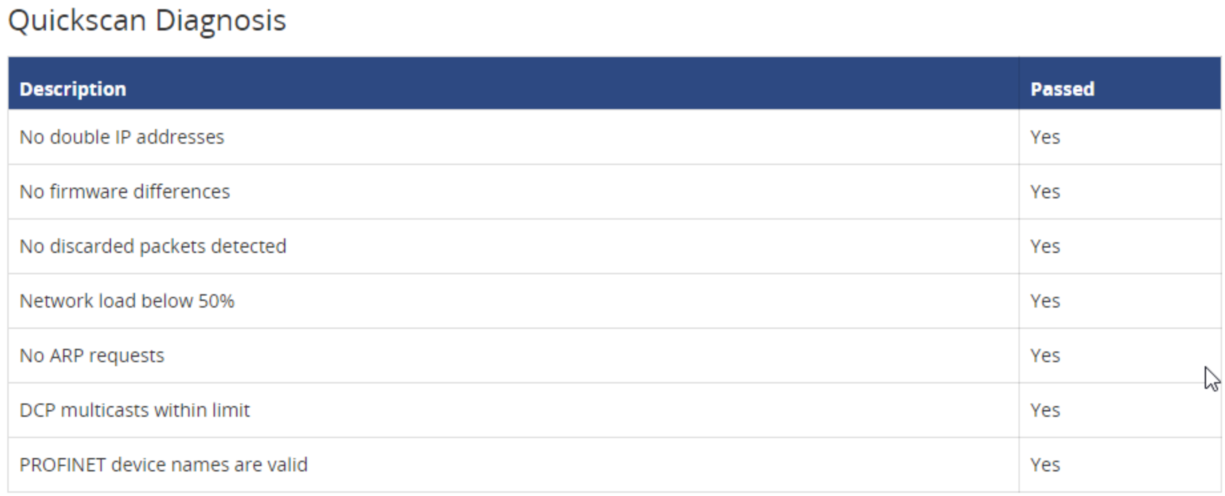
PNT Pro looks good, from their website, and is certainly a tool that deserves a look. However, there is one aspect that bothers me a bit – it has an option of basing its analysis on a mirrored port. A mirrored port is a function of a managed switch where it will copy all the data going to and from one port, normally the controller, and 'mirror' out another port. I used to be a big fan of port mirroring – I thought it was great. Then, I learnt more about how switches worked and realized that as soon as a switch is having trouble, port mirroring is the first function to have resources dropped. This means that just when you need the information the most is when this is going to break down.

Hilscher has two products, netANALYZER and netIOT Diagnostics. NetANALYZER is a different animal. Like Wireshark, this is strictly a passive monitor. Yes, it provides live list and basic data, but then it goes on and lets the control engineer study the interaction of different control signals in real-time. If you have the problem of something starting at the wrong time periodically, or you need to examine your process timing to see how to speed up production, then this is the tool for you! Will it help you troubleshoot your network? Yes, but that is not its main focus.

Hilscher's netIOT Diagnostics and Indu-Sol PROFINET INspektor NT and PROCENTEC Osiris are very similar. However, Osiris has more features at this point. Below is a comparison:

- netIOT Diagnostics and INspektor have a built-in aggregated TAP (Test Access Point), while Osiris uses an external aggregated TAP called EtherTAP. It is nice having the TAP built-in. However, both of these monitors can be used just as an active monitor. This means that if you just want the active monitor features and do not need the passive ones, you still have to pay for the aggregated TAP in the case of the INspektor and netIOT, but do not in the case of Osiris.
- Osiris's EthernetTAP can be used directly by Wireshark, while INspektor and netIOT built-in aggregated TAP can only be used by those packages.

- Osiris can save Wireshark captures based on events. You can then download them to look at them in more detail. This is very useful for advanced troubleshooting. Both INspektor and netIOT cannot do this.
- INspektor has a separate program that can pull information from several INspektors. This is nice, but I could not find an OPC or MQTT support in the product? Osiris has both OPC and MQTT, which fits better into most plants' information structures.
- NetIOT Diagnostics is an Edge computer, so it also has OPC and MQTT built-in. This is an interesting product since it is two products in one – an Edge computer and a monitor. From a network design point of view, the only question is if you want your network monitor to be the same device that also collects all your key data and passes it up to your higher systems?
- Osiris was the first to come out with a commissioning wizard that followed the PROFINET Commissioning Guidelines. INspektor also added this feature. I could not find any reference to this sort of feature in netIOT. This feature is extremely important when commissioning a PROFINET or EtherNet/IP network since it finds measurements that you need to know but are hard to find any other way. The chart below shows some of the key indicators that Osiris finds:



Quickscan Diagnosis

Description	Passed
No double IP addresses	Yes
No firmware differences	Yes
No discarded packets detected	Yes
Network load below 50%	Yes
No ARP requests	Yes
DCP multicasts within limit	Yes
PROFINET device names are valid	Yes

- Osiris has Delphi, a digital assistant who shares PROCENTEC's 20 years of network troubleshooting knowledge. I think of it as help on steroids. In other words, we are talking about help that actually helps you. Both netIOT and INspektor have some help built into the software, but as near as I could tell, they were 'normal' help. This comment is really more of a complement to Delphi than a negative to netIOT and INspektor. Delphi's help is quite exceptional, based on my experience.
- Osiris and netIOT support PROFINET, EtherNet/IP, Modbus TCP and standard Ethernet. INspektor supports PROFINET and EtherNet/IP but not at the same time.

One problem that exists with all of these tools is that to use them you still need to have a certain level of Training. Granted, Osiris has Delphi, which is a big step forward. However, even the most user-friendly tool needs the user to understand certain basic terms. Therefore, the last element is Training.

Summary of Chapter 4

Although IT has great monitors for Ethernet, it is best to have monitors designed for OT because of the difference between OT and IT requirements. We have looked at the major players, and they were all good. At present, Osiris by PROCENTEC appears to be in the lead. Even with great tools, staff training is still required to understand what is going on. In the last chapter, we will look into the future.

Chapter 5

Conclusion and Future Direction

Conclusion

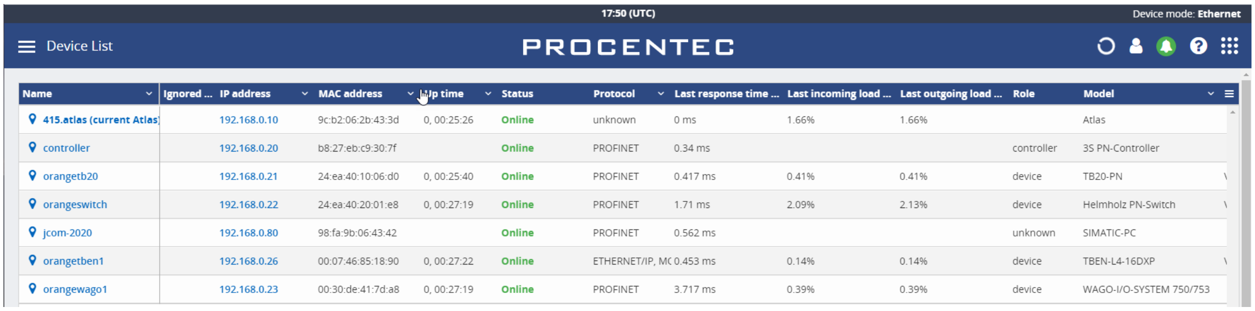
OT has come a long way since the first proprietary serial protocols and has adapted to many technological changes. The convergence of OT and IT is one of the most challenging ones. IT has a lot to offer OT. However, OT and IT have very different requirements.

OT needs to know:

- Who is on the network
- Has anyone joined or dropped off the network
- Any packet losses
- What are the update times and jitter
- What is the network loading
- Any diagnostic messages

Many monitors on the market will provide this information. It is best to use one specifically designed for OT since IT and OT have different objectives. The monitors can provide both active and passive monitoring. It is up to the end-user to decide what type they want or if they want both.

Osiris by PROCENTEC is currently leading the market for Industrial Ethernet monitors. With all of the Ethernet Monitors, having an educated staff is key in their successful deployment.



Name	Ignored ...	IP address	MAC address	Up time	Status	Protocol	Last response time ...	Last incoming load ...	Last outgoing load ...	Role	Model
415.atlas (current Atlas)		192.168.0.10	9c:b2:06:2b:43:3d	0, 00:25:26	Online	unknown	0 ms	1.66%	1.66%		Atlas
controller		192.168.0.20	b8:27:eb:c9:30:7f		Online	PROFINET	0.34 ms			controller	3S PN-Controller
orangetb20		192.168.0.21	24:ea:40:10:06:d0	0, 00:25:40	Online	PROFINET	0.417 ms	0.41%	0.41%	device	TB20-PN
orangeswitch		192.168.0.22	24:ea:40:20:01:e8	0, 00:27:19	Online	PROFINET	1.71 ms	2.09%	2.13%	device	Helmholz PN-Switch
jcom-2020		192.168.0.80	98:fa:9b:06:43:42		Online	PROFINET	0.562 ms			unknown	SIMATIC-PC
orangetben1		192.168.0.26	00:07:46:85:18:90	0, 00:27:22	Online	ETHERNET/IP, MC	0.453 ms	0.14%	0.14%	device	TBEN-L4-16DXP
orangewago1		192.168.0.23	00:30:de:41:7d:a8	0, 00:27:19	Online	PROFINET	3.717 ms	0.39%	0.39%	device	WAGO-I/O-SYSTEM 750/753

Figure 9: Osiris showing a device list of who is on the network

Future Direction

Now is the time to get out our trusty Industrial Ethernet Crystal ball and look into the future. The only problem is that I do not have a crystal ball. However, I have noticed some trends in the industry that I am quite sure will be continuing:

- Industrial networks are getting more complicated
- End-users are supporting more systems
- fewer people in maintenance

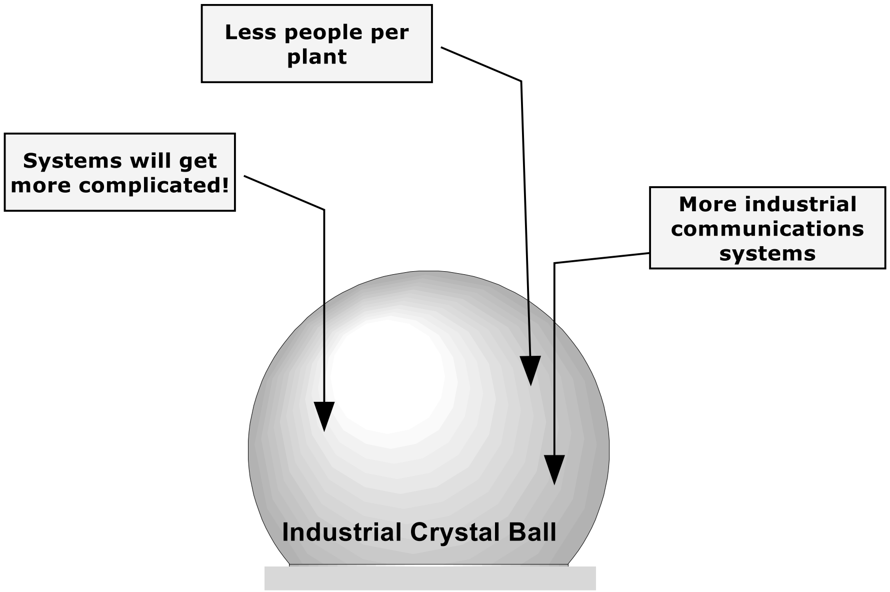

Less people per plant
Systems will get more complicated!
More industrial communications systems
Industrial Crystal Ball

Figure 10: My industrial crystal ball

Maintenance people have to support more systems with fewer people, guaranteeing that their level of knowledge on each system must drop – one person can only know so much. When we add this trend to the first one, that the networks are getting more complicated, then it is easy to see that we are heading for trouble.

The solution is to put monitors in place that will take the load off maintenance. Then have the training in place for maintenance staff and experts ready to help if needed. The monitors will have to provide the required information in a simple format. Then it will have to highlight when things go wrong and have simple easy to follow explanations on what it means and what to do. When difficult issues occur, you need to know people who you can pull in to solve those problems fast.

In this paper, I have outlined many great monitors on the market. Osiris by PROCENTEC is currently in the lead. Each user should look at the different options and decide which one is best suited for their needs.

There are also many training and consulting companies to help end-users with their networks. Companies such as PROCENTEC in the Netherlands, JCOM Automation Inc. in Canada and the USA, Control Specialists Ltd. in the UK, and IDX in South Africa to name a few, are ready to help. The ones that I have listed are all certified PROFINET competence and training centers with additional expertise in EtherNet/IP and Modbus TCP.

Maintenance staff can no longer be experts in all of these systems. However, with a user-friendly monitor in place, proper basic training and an expert on speed dial, maintaining your system will be ensured.

By: James Powell, P.Eng.

About the author: James Powell, P.Eng., is the Principal Engineer and owner of JCOM Automation Inc. in Peterborough, Ontario, Canada. James is an expert in PROFIBUS, PROFINET, EtherNet/IP, Modbus and HART. He has written 'HART Communication Protocol – a practical guide' and co-authored 'Catching the Process Fieldbus – An introduction to PROFIBUS and PROFINET'. He has over 30 years experience with industrial communications and has presented technical training in China, Chile, Argentina, Ecuador, USA, Canada, UK, Germany, and the Netherlands. He is a certified PROFIBUS DP, PA, PROFINET network engineer and PROFIBUS System Design Engineer. You can contact him at jamesp@jcomautomation.ca.