Real-Time Performance of Industrial Ethernet in Field Devices

Abstract

Field devices must continuously perform their tasks on-time under a myriad of manufacturing conditions. These conditions affect device up-time and maintenance actions that impact the factory’s bottom line. Everyone is familiar with how temperature, humidity, vibration, and EMC can affect a field device. But there is one condition that has received little attention to date: network traffic loading. Field devices must continue to operate flawlessly in the presence of a wide range of network traffic conditions. Yet little testing is done to ensure devices will be able to operate under varying network traffic loads. As Industrial Ethernet gains acceptance, network loading will invariably increase over time further impacting device performance. This white paper shows how network traffic influences field device behavior and how to measure its performance.

Industrial Ethernet Network Traffic Components

There can be many different types of network traffic on the wire in an Industrial Ethernet environment. In addition to the cyclic and acyclic components of a particular Industrial Ethernet protocol, there are other sources of standard Ethernet traffic including network management and diagnostics, and network applications. Figure 1 (a) depicts these components and how they may vary over time.
Factory automation systems have historically been connected using direct point to point wiring or serial fieldbuses. In both of these situations the control signals are the only signals present on the wire. This is not true with Industrial Ethernet where the control signals have to coexist with other network traffic. Due to the added complexity and unpredictable nature of traffic on Ethernet networks, designing and testing such systems is much more complex than with simple serial bus interfaces [1]. A key reason for switching to an Ethernet based network is that the factory can be made more intelligent by way of the additional network applications and data management. An example that illustrates this benefit is the desire to archive quality data [2]. On an Ethernet network, machine tools in an assembly line can send their data over the network to an archive server for retrieval and analysis. This data would need to pass through the control network on its way to the archive server which may be located at the Enterprise level. The frequency and nature of the quality data can vary greatly – some machine tools and production lines may require archival of torque data on every action – potentially causing a wide variability in network loading.

Additional network traffic is generated during network configuration. Each field device must understand the network around it, so management traffic is constantly travelling around the network updating network topology information. When a field device anywhere in the factory is replaced, this will cause an increase in network management traffic as the devices reconfigure. Web servers inherent in many field devices provide a convenient means to configure, read status and perform updates and are the source of additional network application traffic.

Any component of network traffic can cause temporary heavy network load conditions. Figure 1 (b) depicts a surge in network traffic. Such a surge can be caused by any number of events in the system. One common event is an ARP Burst, or “ARP storm”. This can be caused by simply plugging a maintenance PC into an otherwise stable network. In order to discover the
devices on the network, such a PC will often send an identity broadcast request to the network. Every device will hear this broadcast but no device can respond until it updates its ARP table to contain the PC's IP address. So every device will simultaneously send an ARP request broadcast to learn the PC's IP address, causing the network traffic load to surge. Surges can also be caused by faulty equipment [3] and by Denial of Service attacks (DoS).

Despite the variability of network traffic, modern control systems are expected to continue to operate flawlessly [2].

![Network Management & Diagnostics](image)

**Figure 1 (b) – Network Traffic Components in Industrial Ethernet, Network Load Surge**

**Network Topology**

Industrial Ethernet networks utilize a combination of star, line, redundant star, and ring topologies to connect field devices to controllers. In this paper a line topology is used rather than a ring or star topology. By placing the test device at the Beginning-Of-Line (BOL), a line topology provides load conditions similar to a ring topology without the redundancy protocol. Placing the test device at the End-Of-Line (EOL) provides similar load conditions to a star topology. A device at the Beginning-Of-Line sees not only its own traffic, but also all of the traffic of the devices down the line. A device at the end-of-line does not see any of the upstream traffic, except broadcast messages, so the network load it sees is less than if it were at the Beginning-of-Line. Figure 2 shows the network topology used for testing field devices. For each test case a network tap is placed in line with the device under test (DUT) to capture network traffic to and from the DUT. The tap provides network bus loading (percentage) and an accurate (+/- 10 nS) timestamp of each captured data packet. This data is post processed using the IENetP tool provided by the National Institutes of Standards and Technology (NIST) to provide a time plot and a statistical look at the DUT’s performance.
Network Traffic

For the purpose of the tests presented in this white paper, two types of network traffic components were used: (1) Industrial Ethernet Cyclic Data, and (2) Network Management and Diagnostics. These components comprised eight traffic scenarios which are defined in Table 1. Industrial Ethernet Cyclic Data was used in all eight scenarios, and different types of Network Management traffic were injected for each of the scenarios [4].

Test Procedure

Two networks were built – one for Profinet testing using a Siemens PLC and one for EtherNet/IP testing using a Rockwell PLC. These networks were configured as shown in Figure 2. Each PLC and all DUT’s were configured to exchange cyclic I/O data at a rate of 2 ms. This cyclic I/O traffic flow was maintained for the duration of the testing. Commercially available EtherNet/IP and Profinet I/O devices were purchased from different vendors and tested in these networks. Each I/O device (DUT) was exposed to all 8 traffic scenarios in both the End of Line (EOL) topology and Beginning of Line (BOL) topology configurations.

Figure 2 – Network Topology for Network Load Testing
Table 1 – Definition of Network Load Test

<table>
<thead>
<tr>
<th>Scenario #</th>
<th>Traffic Scenario</th>
<th>Purpose</th>
<th>Load Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cyclic Traffic Only</td>
<td>Establish device baseline performance</td>
<td>No specific background traffic present, I/O data flowing at 2 ms cyclic rate. This I/O traffic level was maintained throughout the testing.</td>
</tr>
<tr>
<td>2.</td>
<td>Steady State Managed</td>
<td>Test basic network traffic management</td>
<td>Additional basic network traffic, ARP, DHCP, ICMP, etc.</td>
</tr>
<tr>
<td>3.</td>
<td>Steady State Unmanaged</td>
<td>Test response to multicast streams not directed to device under test (DUT)</td>
<td>Same as steady state managed but add 1800 packets/second multicast traffic background</td>
</tr>
<tr>
<td>4.</td>
<td>Burst Managed</td>
<td>Test DUT response to a real world level of burst broadcast traffic</td>
<td>Same as steady state managed but add repeated ARP bursts of 240 packets at 4000 packets/second (60 ms bursts)</td>
</tr>
<tr>
<td>5.</td>
<td>Burst Unmanaged</td>
<td>Test DUT response to composite tests</td>
<td>All of the above, basic network traffic, multicast stream and ARP bursts</td>
</tr>
<tr>
<td>6.</td>
<td>30% Bus Utilization</td>
<td>Test DUT response to low volume of continuous burst broadcast traffic</td>
<td>Send sufficient ARP broadcast traffic to create a continuous bus utilization of 30% of the 100M bps bandwidth.</td>
</tr>
<tr>
<td>7.</td>
<td>60% Bus Utilization</td>
<td>Test DUT response to medium volume of continuous burst broadcast traffic</td>
<td>Send sufficient ARP broadcast traffic to create a continuous bus utilization of 60% of the 100M bps bandwidth.</td>
</tr>
<tr>
<td>8.</td>
<td>95% Bus Utilization</td>
<td>Test DUT response to high volume of continuous burst broadcast traffic</td>
<td>Send sufficient ARP broadcast traffic to create a continuous bus utilization of 95% of the 100M bps bandwidth.</td>
</tr>
</tbody>
</table>
Three PCs were used for network traffic generation and analysis; one for the Network Load Generator, one for the Network Noise Generator, and one for the Network Tap. The Network Load Generator created traffic for scenarios 2 through 5, and the Network Noise Generator was added to create traffic for scenarios 6 through 8.

Field devices for Profinet and EtherNet/IP were tested using the same basic test procedure. The steps for testing a particular device were as follows:

1. Test at the Beginning-of-Line (BOL):
   a. Connect the I/O devices with the necessary topology; placing the DUT at BOL and connect the network TAP in line with the DUT.
   b. Start the I/O data flowing by connecting a network controller (PLC) to the I/O devices. For the devices that support it use a 2 ms cyclic rate, for other devices, (that cannot run this fast), use the fastest rate supported by the device.
   c. While monitoring the system to detect connection loss or I/O timeouts collect at least 60 seconds of network traffic for analysis.
   d. Set up the network background traffic level as appropriate (see Table 1).
   e. While monitoring the system to detect connection loss or I/O timeouts collect at least 60 seconds of network traffic for analysis.
      • If the device loses connection or it experiences a time out, record the event as failure.
   f. Repeat steps c and d for traffic scenarios 2 through 8.

2. Test at the End-of-Line (EOL):
   a. Connect the I/O devices with the necessary topology; placing the DUT at (EOL) and connect the network TAP in line with the DUT.
   b. Start the I/O data flowing by connecting a network controller (PLC) to the I/O devices. For the devices that support it use a 2 ms cyclic rate, for other devices, (that cannot run this fast), use the fastest rate supported by the device.
   c. While monitoring the system to detect connection loss or I/O timeouts collect at least 60 seconds of network traffic for analysis.
   d. Set up the network background traffic level as appropriate (see Table 1).
   e. While monitoring the system to detect connection loss or I/O timeouts collect at least 60 seconds of network traffic for analysis.
      • If the device loses connection or it experiences a time out, record the event as failure.
   f. Repeat steps c and d for traffic scenarios 2 through 8.
3. Analyze Results
   a. Using the NIST IENetP tool, post process the collected network traffic data to compute the statistical performance data and to create performance graphs. Use a protocol appropriate Wireshark filter to isolate the cyclic I/O data traffic from the background.
   b. Plot DUT performance across all 8 traffic scenarios.

The next section describes how the field devices performed under the test procedure described above.

Field Device Performance

The performance of each device was assessed by analyzing packet response for a target 2 ms cycle time. Statistics were generated from the traffic capture files produced by the test procedure for each of the traffic scenarios and network positions for the supported protocol. A scatter plot of the measured packet performance over time was plotted along with a histogram of the device’s actual packet performance for the measured time period. The product of this analysis was a set of up to 16 plots for each DUT - 8 for the BOL network position and 8 for the EOL position.

An example plot is shown in Figure 3. This particular device was tested on an EtherNet/IP network, at the BOL position, using an I/O cycle time of 2 ms while injecting network traffic from Traffic Scenario 6. It exhibited the following characteristics:

- Mean Packet Response: 2.009 ms
- Minimum Packet Response: 1.387 ms
- Maximum Packet Response: 3.078 ms
- Standard Deviation: 0.127 ms

There are 7 other plots for this device corresponding to the 7 other traffic scenarios at the BOL position. There are another 8 plots for this device for the EOL traffic scenarios. What is interesting to note about this device is that it could not hold a 2 ms cycle time. It was off, on average by 9 µs and had 125 µs of jitter.

Figure 4 shows a device on a Profinet network. It was also tested at the BOL position, using an I/O cycle time of 2 ms while injecting network traffic from Traffic Scenario 6:

- Mean Packet Response: 2.000 ms
- Minimum Packet Response: 1.54 ms
- Maximum Packet Response: 2.833 ms
- Standard Deviation: 0.367 ms

Again, there are 7 other plots for this device corresponding to the 7 other traffic scenarios at the BOL position. This device was able to hold a 2 ms cycle time but had 367 µs of jitter.
Figure 3 – Example Performance Plot for a device on an EtherNet/IP network

Figure 4 – Example Performance Plot for a device on a Profinet network
Overall device performance was assessed by looking at the statistics across all traffic scenarios. The Mean, Minimum, Maximum, and Standard Deviation of the packet response were plotted against the traffic scenarios for BOL and EOL network positions. Baseline performance was plotted first, followed by the other traffic scenarios and concluding with the 95% Bus utilization case.

Figure 5 shows these overall results for the device plotted in Figure 3 in an EtherNet/IP network. This device (in Figure 5) has noticeably different response when in the BOL vs. the EOL position and performs better at the EOL position for the most part. Also, the device did not disconnect from the network even at high traffic loads.

Figure 6 shows these results for the device plotted in Figure 4 using a Profinet network. The device (in Figure 6) performs fairly consistent for both BOL and EOL network positions until 60% Bus utilization is reached. At that point the device disconnects from the network when in the BOL position.

Additional devices were tested for both EtherNet/IP and Profinet. Another 3 devices were tested in the EtherNet/IP network, and another 2 devices were tested in the Profinet network. The same statistics and plots shown in Figures 3 through 6 were generated for each of these devices.

Figure 5 – Performance of a device on an EtherNet/IP network across all traffic scenarios
The devices were also compared to each other by looking at the worst case performance across all the traffic scenarios. This comparison is shown in Figures 7 and 8 by plotting the Maximum Packet Response for each device against the traffic load. For both protocols, there was a wide range of performance and many devices completely disconnected from the network when under stress. The device based on Innovasic’s RapID Platform solution had consistently good results in both Profinet and EtherNet/IP networks regardless of the traffic scenario and it never disconnected from the network. Innovasic’s RapID platform employs a technology called PriorityChannel™ enabling it to maintain consistent performance from the wire all the way to the application layer under all stress conditions (www.innovasic.com/prioritychannel).
Figure 7 – Performance of all devices on an EtherNet/IP network across all traffic scenarios

Figure 8 – Performance of all devices on a Profinet network across all traffic scenarios
Conclusion

There are many traffic components in an Industrial Ethernet network regardless of the type of protocol. Many of these components are necessary for network management and diagnostics, so it is incorrect to conclude that industrial networks are pristine and only contain traffic relevant to the task at hand for controllers and field devices. In addition, it is clear that devices can behave very differently in response to the various traffic conditions found on a typical network. Some devices seem immune to network loading and others are severely affected, some even disconnecting as the traffic load increases. This is the case regardless of whether the network is Profinet or EtherNet/IP.

When selecting an I/O device for the factory floor there is clearly much more to consider than the functional features alone. While the published specifications rarely reflect a device’s true performance capabilities, it is relatively easy to create a testing environment that can bring these things into the light. This testing shows that not all devices respond the same to varying network loads. Care must be taken when implementing a solution in order to achieve a consistent performance level across different network traffic conditions. To discover these issues while trying to achieve a production run is much too late.

References