Data Storm Vulnerability

1.0 Data Storm Background

A Data Storm event is where excessive and/or unrelated network traffic creates a "processing overload" condition that degrades the performance and timely response of communications. Data Storm events cause severe delays, missing data, or corruption of important and sometimes critical network data.

A Data Storm event can be malicious in nature, but can also be created by unique hardware/software failures or poor network design. The severity and impact depends specifically on the network architecture and the device(s) involved, but can range from simple inconvenience to serious system shutdowns. This event may cause a system or specific device to operate slowly, intermittently, or even to fail completely.

In essence, high traffic conditions must be minimized and eliminated to ensure robust network response and operation. This is especially critical for control-related communication networks. The network design and architecture is the primary protection from Data Storm events and must include the following considerations.

- Proper network architecture that includes firewalls, traffic segmentation, and traffic control
- Careful network partitioning that includes separation between non-critical and critical networks.
- Careful access controls and permissions for both plant and control networks.
- Careful selection of network devices including network routers, switches, and industrial controllers.
- Redundant communication paths where needed.

Each device on the network offers a different level of protection from Data Storm events. A serial communication link that is point to point and distance limited is less susceptible than a large plant-wide Ethernet network. A master that polls a network device for information is less susceptible that a master that is continually interrupted on incoming packets. Devices that have built-in packet, protocol, address, and data verification will also be more robust during Data Storm events.

2.0 Woodward MicroNet & MicroNet TMR

For Woodward Ethernet & SIO modules, the MicroNet CPU will poll the module for new data at specific rategroup intervals. Woodward Serial and Ethernet modules are designed to detect specific hardware and protocol related failures that can often be related to Data Storm events. When an error is detected, it will be flagged and the data packet will not be used. If errors persist long enough, then a Link Error failure will be annunciated.

2.1 ModBus Communications (Ethernet & Serial)

Woodward ModBus communication links over Ethernet & Serial ports will detect the following issues. The application software can take appropriate action as well as notify the operator that such conditions exist.

- Ethernet & SIO module hardware faults
- LINK Error: No response within a selected timeout value.
- ILLEGAL FUNCTION code detected.
- ILLEGAL DATA ADDRESS referenced in data field
- ILLEGAL DATA VALUE where the amount of data requested was too large
- CHECKSUM ERROR where the message checksum is invalid.
- GARBLED MESSAGE where the received data packet was invalid.
- UNSOLICITED MESSAGE received from slave.
- BAD Function Code in a response message.
- BAD Address in a response message:
- NO SLAVE RESPONSE where the slave did not respond.
- Internal code or System error.

2.2 Additional Serial I/O module faults

SIO module hardware will detect the following additional issues. The application software can take appropriate action as well as notify the operator that such conditions exist. The Woodward CPU will poll the SIO module for new data.

- Module hardware faults
- Parity Error, Buffer Overrun Error, Framing Error, Receive Queue Overrun Error, Input String too Long

3.0 Test Results

The MicroNet TMR system was configured with a DNA Ethernet module in both Kernel B and Kernel C. The application was setup with a UDP ModBus Master in kernel B and a UDP ModBus Slave in kernel C. The link errors were monitored with a latch block.

3.1 Data Storm Test

A Spirent Smartbits 200 Ethernet Performance Analysis System was used to create a broadcast Data Storm.

The Smartbits was setup to transmit data at the fastest rate of 960 nanoseconds between packets with a varying data length. The connection was configured at 100 MB with full duplex.

The Smartbits port was connected through an Ethernet switch to both of the DNA Ethernet modules.

The data storm was enabled and allowed to bombard the DNA modules for an hour. During this test, the data storm was able to create link errors on the ModBus connection, but the system control operation was not interrupted.

3.2 Vulnerability Test

A Nessus® vulnerability scanner was also used to test the interface security of the DNA Ethernet Module. Nessus is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis of your security posture. A Nessus Client scanner was used to perform a full security test and report of both system DNA Ethernet modules in both B and C kernels.

The Nessus vulnerability scan test resulted in the following report:

- No interruption of system control
- High security attack vulnerability rating
- High connection bombardment rating

Attached is the scan report.

Nessus Scan Report TMR 040.mht