Woodward Governor Company
1000 East Drake Road
P.O. Box 1519
Fort Collins, CO 80522-1519 USA
Tel: 970-482-5811
Fax: 970-498-3058

April 30, 2009

SUBJECT: MicroNetTMR 68040 Data Storm Susceptibility

TO WHOM MAY CONCERN:

The Woodward MicroNetTMR platform with CPU68040 modules and DNA based Ethernet modules installed has been verified to not be susceptible to Data Storm events. Through simulated Data Storm testing, it has been proven that Data Storm events have no effect on system operation, and only temporarily affect unit communications.

The MicroNetTMR platform has multiple layers of protection from network communication issues such as Data Storm events, sent garbled messages, and incorrect instructions. The MicroNetTMR platform is architected such that its CPU modules and communication modules have separation through its VME backplane. This processor to processor separation, coupled with the manner the main CPU module polls each Ethernet and SIO module for new data at specific rate group intervals, coupled its communication error detection capability, make the MicroNetTMR platform very resistant to Data Storm type of communication errors.

MicroNet Serial and Ethernet modules are designed to detect specific hardware and protocol related failures that can often be related to Data Storm events. When such communication errors are detected, the CPU module is flagged and the data packet is not be used. If errors persist long enough, a Link Error failure is annunciated, and the application program can be configured to inhibit CPU module from polling the specific communication port. Additional messages from the data storm received by the DNA module are then discarded and never passed to the main CPU.

Woodward ModBus communication links over Ethernet & Serial ports detect the following issues allowing the application program to disable the port and ignore a storm of instructions.

- Hardware faults
- LINK Errors: No response within a selected timeout value.
- ILLEGAL FUNCTION codes detected.
- ILLEGAL DATA ADDRESSES referenced in data field
- ILLEGAL DATA VALUES where the amount of data requested was too large
- CHECKSUM ERRORS where the message checksum is invalid.
- GARBLED MESSAGES where the received data packet was invalid.
- UNSOLICITED MESSAGES received from slave.
- BAD Function Codes in a response message.
- BAD Addresses in a response message:
- NO SLAVE RESPONSE where the slave did not respond.

Woodward followed industry standard “Spirent SmartBits Ethernet Performance Analysis system” guidelines to simulate Data Storm events into the MicroNetTMR platform. For these specific system tests a time period of 960 nanoseconds was used between packets and varying packet data sizes were broadcasted into the MicroNetTMR’s Ethernet ports. During

these tests, the data storm was able to create link errors on the Ethernet communication ports, but system control operation was not interrupted.

Additionally, a Nessus® vulnerability security scanner was used to test the interface security of the MicroNetTMR's DNA Ethernet Module's Ethernet communication port. Nessus is the world-leader in active security scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis of your security posture. This Nessus security scan test performed on the MicroNetTMR's Ethernet communication port resulted in the following findings:

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

For more detailed testing and report information please refer to Woodward report 89546-R79.

Regards,

Rich Kamphaus
Turbomachinery Controls Product Line Manager
Woodward - (rich.kamphaus@woodward.com)