UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

April 17, 2007

NRC INFORMATION NOTICE: 2007-15: EFFECTS OF ETHERNET-BASED, NON-SAFETY RELATED CONTROLS ON THE SAFE AND CONTINUED OPERATION OF NUCLEAR POWER STATIONS

ADDRESSEES

All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice (IN) to alert licensees about recent operating experience related to the effects of potential interactions and unanticipated failures of ethernet connected non-safety equipment on the safety and performance capability of nuclear power stations. NRC expects that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this IN are not NRC requirements; therefore, no specific action or written response is required.

DESCRIPTION OF CIRCUMSTANCES

On August 19, 2006, operators at Browns Ferry, Unit 3, manually scrammed the unit following a loss of both the 3A and 3B reactor recirculation pumps. Plant procedures following the loss of recirculation flow required the manual scram. Immediate loss of the recirculation flow placed the plant in a high power, low flow condition where core thermal hydraulic stability problems may exist at boiling-water reactors (BWRs). Generally, intentional operation in this condition, of high power and low flow, is not permitted. Although some BWRs are authorized for single loop operation, sudden loss of even one pump could present the plant with the same stability problems and could result in the reactor protection system initiating a shutdown of the plant.

The initial investigation into the dual pump trip found that the recirculation pump variable frequency drive (VFD) controllers were nonresponsive. The operators cycled the control power off and on, reset the controllers, and restarted the VFDs. The licensee also determined that the Unit 3 condensate demineralizer controller had failed simultaneously with the Unit 3 VFD controllers. The condensate demineralizer primary controller is a dual redundant programmable logic control (PLC) system connected to the ethernet-based plant integrated computer system (ICS) network. The VFD controllers are also connected to this same plant

ICS network. Both the VFD and condensate demineralizer controllers are microprocessor-based utilizing proprietary software.

The licensee determined that the root cause of the event was the malfunction of the VFD controller because of excessive traffic on the plant ICS network. Testing by site personnel performed on the VFD controllers confirmed that the VFD control system is susceptible to failures induced by excessive network traffic. The threshold levels for failure of the VFD controllers due to excessive network traffic, as determined by the on-site testing, can be achieved on the existing 10-megabit/second network. The NRC staff's review of industry literature and test reports on network device sensitivity, and the threshold levels for such failures, confirmed these testing results. The licensee could not conclusively establish whether the failure of the PLC caused the VFD controllers to become nonresponsive, or the excessive network traffic, originating from a different source, caused the PLC and the VFD controllers to fail. However, information received from the PLC vendor indicated that the PLC failure was a likely symptom of the excessive network traffic.

To ensure that excessive network traffic will not cause future Unit 3 VFD controller malfunctions, the licensee disconnected these devices from the plant ICS network before restart. The licensee also disconnected the Unit 2 VFD controllers from the plant ICS network.

Licensee corrective actions included (1) developing a network firewall device that limits the connections and traffic to any potentially susceptible devices on the plant ICS network and (2) installing a network firewall device on each unit's VFD controller and condensate demineralizer controller. The Browns Ferry Unit 3 event is discussed in Licensee Event Report 05000296/2006-002, dated October 17, 2006, Agencywide Documents Access and Management System, Accession No. ML062900106.

BACKGROUND

Ethernet is one technology used for local area networking (LAN) of many different types of digital devices such as computers, process controls, modems and PLCs. This allows many of these devices to transfer data over a common communications cable, typically coaxial cable, or special grades of twisted pair wire. It is the most widely used LAN technology today.

A data packet is a basic unit of data in a networked environment. In basic networks, data packets are broadcast, meaning sent to each network device, rather than to one specific device. To function properly, a device must be able to effectively handle the broadcast data packets it receives.

A key point is that all network devices must allocate time and resources to read and interpret each broadcasted data packet, even if the packet is not intended for that particular device. Excessive data packet traffic on the network may cause connected devices to have a delayed response to new commands or even to lockup, thereby, disrupting normal network operations. This excessive network traffic is sometimes called a broadcast (or data) storm.

A firewall is a mechanism used to control and monitor data traffic to and from a network, or device, for the purpose of protecting devices on a network. In effect, it is a filter that blocks

unwanted network traffic and limits the amount and type of communication flow. A firewall can act as an intrusion detection system by identifying data packets that are denied access, recognizing data packets specifically designed to cause problems, or reporting unusual (including excessive) traffic patterns, and many other security-based features.

The reason the licensee at Browns Ferry investigated whether the failure of one device, the condensate demineralizer PLC, may have been a factor in causing the malfunction of the VFD controllers is that there is documentation of such failures in commercial process control. For instance, a memory malfunction of one device has been shown to cause a data storm by continually transmitting data that disrupts normal network operations resulting in other network devices becoming "locked up" or nonresponsive. A network found to be operating outside of normal performance parameters with a device malfunctioning can effect devices on that network, the network as a whole, or interfacing components and systems. The effects could range from a slightly degraded performance to complete failure of the component or system. Major contributors to these network failures can be the addition of devices that are not compatible, network expansion without a procedure and a overall network plan in place, or the failure to maintain the operating environment for legacy devices already on the network.

DISCUSSION

While only non-safety related network devices became nonresponsive at Browns Ferry Unit 3, it is important to protect both safety-related and non-safety related devices on the plant network to ensure the safe operation of the plant. The August 19, 2006, transient unnecessarily challenged the plant safety systems and placed the plant in a potentially unstable high-power, low-flow condition. The potential safety implications for future similar events would depend on the type of devices that are connected to the plant ethernet. Careful design and control of the network architecture can mitigate the risks to plant networks from malfunctioning devices, and improper network performance, and ultimately result in safer plant operations.

CONTACT

This IN requires no specific action or written response. Please direct any questions about this matter to the technical contact listed below or the appropriate Office of Nuclear Reactor Regulation project manager.

/RA by TQuay for/

Michael J. Case, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Technical Contact: Royce D. Beacom, NRR
301-415-2781
E-mail: rdb1@nrc.gov

Note: NRC generic communications may be found on the NRC public Web site, http://www.nrc.gov, under Electronic Reading Room/Document Collections.