

Tofino™ Application Note -AN9201



Securing Redundant Communications between an Emergency Shutdown System and a Honeywell Experion System

This application note describes how a petroleum refinery used the Tofino™ Industrial Security Solution to provide secure communications between a Triconex™ Emergency Shutdown (ESD) system and a Honeywell Experion™ process control system. It also explains the use of the Tofino™ system in redundant networks, techniques for grouping large numbers of identical devices in “networks” and the management of nuisance alarms generated by unwanted multicast traffic.

Background

Many ESD systems are interfaced to process control systems using either serial or Ethernet-based communications. This connection allows both systems to share information concerning the state of the process and provide better safety and operations management. However, it also introduces the possibility of security events (such as viruses or Denial of Service (DoS) attacks) migrating from one system to the other, especially in cases where personal computers are being used to program or manage either system. Addressing this risk requires a defense-in-depth solution, where a security firewall carefully monitors and controls all traffic, ensuring only appropriate control traffic is allowed to pass between systems.

Control System Overview

The overall refinery automation strategy in this application note is based on the Honeywell Experion™ control system using C300™ controllers and a Triconex™ TCM Safety Integrated System (SIS). These were interfaced using redundant Modbus and Modbus/TCP communications.

The Experion™ control network utilized the *Honeywell High Security Network Architecture*, a multilayer, Fault Tolerant Ethernet™ (FTE) design with equipment segmented as follows:

- **Level 4** Business network applications such as Manufacturing Execution Systems (MES)
- **DMZ** Nodes that access the process control network as well as the business network
- **Level 3** Advanced control and advanced applications (noncritical control applications)
- **Level 2** Supervisory control and operator interface
- **Level 1** Real time control (controllers and I/O)

Level 1 consisted of four dual-redundant Honeywell C300™ controllers (assigned IP addresses 192.168.1.23 through 192.168.1.30) connected to the Supervisory Control Layer (Level 2), via redundant Honeywell Control Firewalls. Level 2 contained operator consoles in two control rooms, all interconnected using redundant Cisco™ switches. These in turn, were redundantly connected to Level 3 containing the

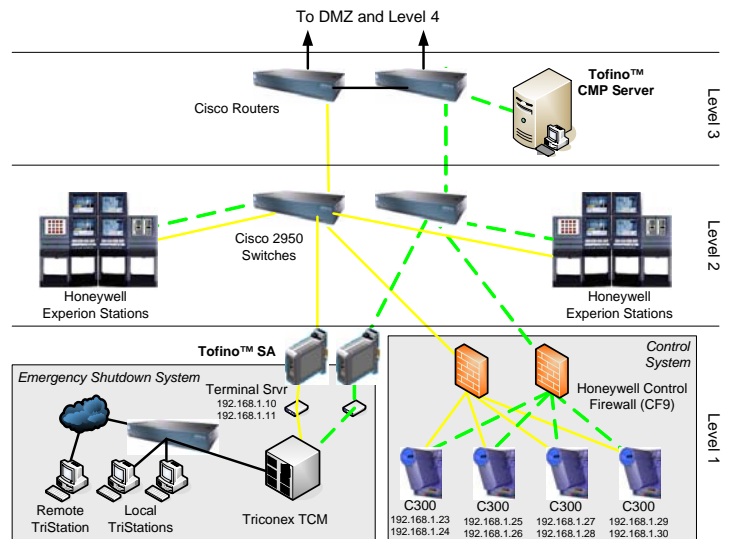


Figure 1: The Control System Network (simplified)



EUROPE (EMEA)
AMERICAS
INTERNATIONAL
ASIA-PACIFIC

Tel: +44 (0)1582 723633
Tel: +1 888 9TOFINO
Tel: +1 780 485 3139
Tel: +65 6 487 7887

E-mail: tofinosupport@mtl-inst.com Web site: www.tofinosecurity.com



Mar 2008

network domain controller and application servers. Above this, resided a Demilitarized Zone (DMZ) to the corporate business network, created using a Cisco ASA™ firewall.

The Triconex™ TCM safety system was configured with dual redundant serial ports supporting the Modbus protocol. Serial communications was converted to Modbus/TCP for the Experion™, using two industrial terminal servers assigned IP addresses 192.168.1.10 and 192.168.1.11.

Tofino™ SA Hardware and CMP Server Installation

Two Tofino™ Security Appliances (SAs) were connected between the Triconex™ terminal servers and the Level 2 Ethernet switches, providing redundant connections between the ESD system and control system. The Tofino™ Central Management Platform (CMP) software was installed on a Windows® 2003 server located in the central control room and connected to the Level 3 switch.

Network Editor Configuration

The first step of the configuration process was to create a network diagram in the Tofino™ CMP that represented the devices and interconnections in the control system. While it is possible to model the entire control network in the Tofino™ CMP, it is only necessary to include those devices that need to have

traffic pass through the Tofino™ SAs. In this case, these devices included the two terminal servers

connected to the Triconex™ system (named ‘Triconex A’ and ‘Triconex B’)

and the eight Honeywell C300™ controllers. To further simplify setup, the eight Honeywell C300 controllers were represented as a single C300 network, resulting in the network diagram shown in Figure 2.

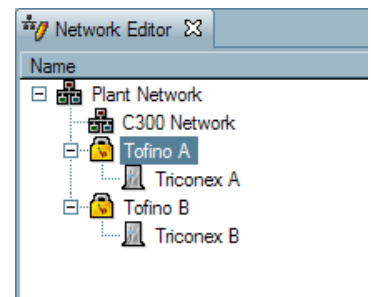


Figure 2: Network Diagram

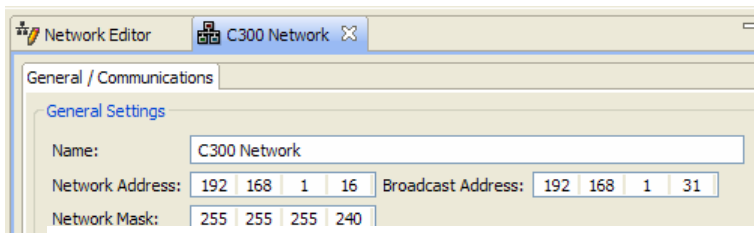


Figure 3: C300 Network IP Address Settings

The ‘C300 Network’ item deserves some comment. Normally, each network device would be represented by a single controller node. However, this would have required eight controller nodes in the network diagram and since IP addresses for the C300’s were contiguous and the rule set for each identical, the refinery chose to represent all of the controllers in a single ‘Network’ node, with address settings as shown in Figure 3. The two Triconex™ nodes were assigned the IP addresses 192.168.1.10 and 192.168.1.11, to match their settings in the field.

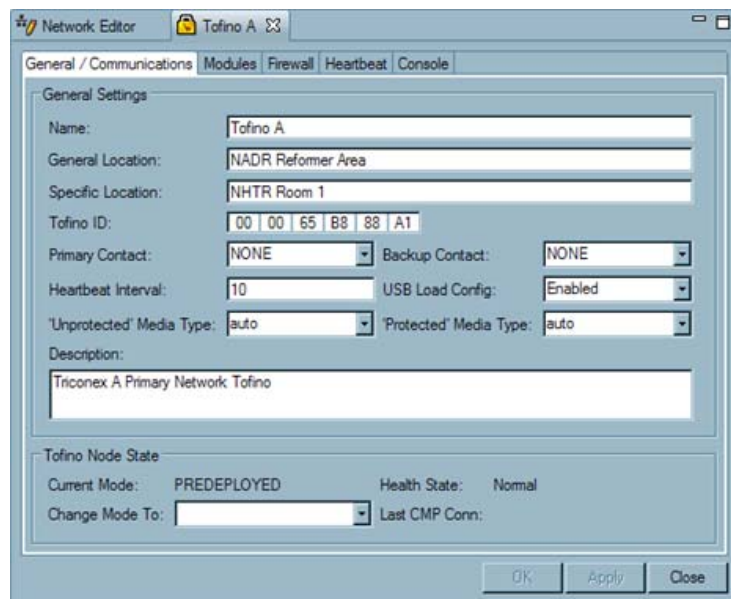


Figure 4: Tofino A’s Communications Configuration

and ‘Triconex B’ were selected as the ‘Contact Device’ for ‘Tofino A’ and ‘Tofino B’, respectively. As well,



EUROPE (EMEA)
AMERICAS
INTERNATIONAL
ASIA-PACIFIC

Tel: +44 (0)1582 723633
Tel: +1 888 9TOFINO
Tel: +1 780 485 3139
Tel: +65 6 487 7887

E-mail: tofinosupport@mtl-inst.com Web site: www.tofinosecurity.com



each Tofino™ SA was changed from ‘Pre-deployed’ mode to ‘Passive’ mode to initiate and secure the Tofino™ CMP to Tofino™ SA communications link. Figure 4 shows the configuration for ‘Tofino A’. Finally, the Firewall Loadable Security Module (LSM) was installed and activated on each of the Tofino™ SAs.

Setting up the Firewall Rules

In order to secure communications between the Triconex™ and Honeywell™ C300s, the Tofino™ Firewall had to be configured to allow Modbus/TCP connections originating from the C300 controllers that were directed to the Triconex™ safety system, and block all other traffic. This was done by creating a firewall ‘rule’ on the Triconex™ icon in the network editor, specifying which other node (in this case the ‘C300 Network’) is allowed to communicate with the Triconex™; what protocol (Modbus/TCP) is permitted; and the direction of the network connection (in this case, incoming to the Triconex™). This was done for both ‘Triconex A’ and ‘Triconex B’ nodes resulting in two Triconex™ firewall tabs, as shown in Figure 5.

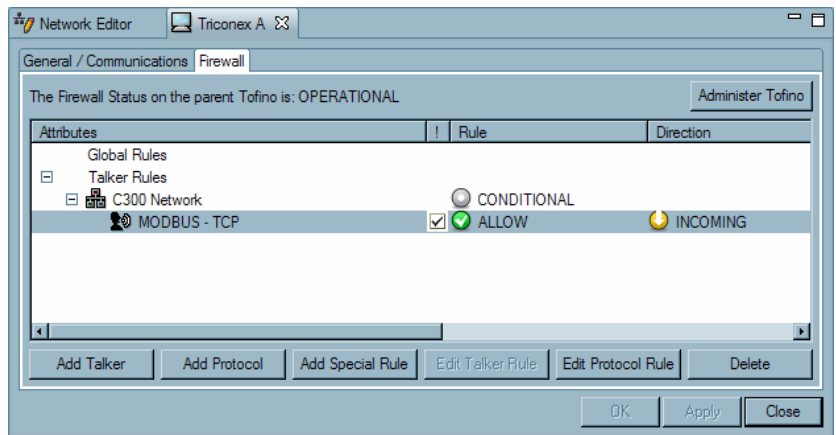


Figure 5: Triconex A's Firewall Configuration

Note that the rule direction was set to ‘Incoming’ because the initiation of the TCP connection was ‘incoming’ with respect to the node where the rule was located. In other words, since the Honeywell™ C300 controllers acted as Modbus masters, only these controllers were allowed to initiate a Modbus/TCP connection to the safety system. The safety system could respond to all Modbus requests, but was not allowed to act as a master and initiate a connection back to the C300 controllers.

Tofino™ Test Mode and System Commissioning

The Tofino™ system offers a mode of operation called Test mode, which allows all network traffic to pass, but reports any traffic that would have been blocked by the firewall had it been in Operational mode as a firewall exception alarm in the Event View of Tofino™ CMP. This mode is ideal for testing firewall rules without accidentally blocking traffic that should be allowed and thus impacting plant operations.

Some example alarms and events are shown in Figure 6. The exception alarms are highlighted, and have a small ‘warning’ icon on the left hand side. Any firewall alarms that say ‘IP Packet DENIED’ signify network traffic that the Tofino™ SA would block when it is in Operational mode. These should be reviewed carefully to ensure that all rules are in place to allow the necessary traffic for proper operation of the process.

Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2007-10-24 16:10:06.355	PERIODIC	NOTICE	FS Tofino	comms	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:10:06.355	PERIODIC	NOTICE	FS Tofino	firewall	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:10:05.104	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet ALLOWED (test) and Logged: Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:09:50.679	PERIODIC	NOTICE	FS Tofino	comms	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:09:50.679	PERIODIC	NOTICE	FS Tofino	firewall	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:09:49.344	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet DENIED (test) and Logged: From 192.168.2.240:13
2007-10-24 16:09:47.151	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet DENIED (test) and Logged: From 192.168.2.159:13

Figure 6: Examples of Alarms Generated During Test Mode



EUROPE (EMEA)
AMERICAS
INTERNATIONAL
ASIA-PACIFIC

Tel: +44 (0)1582 723633
Tel: +1 888 9TOFINO
Tel: +1 780 485 3139
Tel: +65 6 487 7887

E-mail: tofinosupport@mtl-inst.com Web site: www.tofinosecurity.com



Managing Multicast Traffic

Operating the Tofino™ SA in Test mode showed that the firewall rules were correct and the process communications would operate as intended. However, a large number of alarms were being generated by unexpected multicast traffic that was being blocked by the Tofino™ SA. On investigation, it was found that this multicast traffic was originating from several sources, including the Honeywell Fault-Tolerant Ethernet™ (FTE) protocol and Universal Plug & Play (UPnP) traffic from Windows® PCs on the control network.

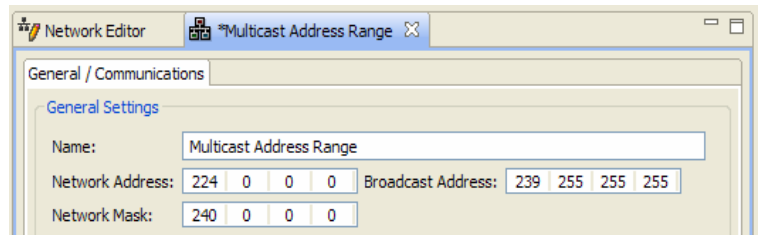


Figure 7: Configuration of “Multicast” Network Node

Since only Modbus/TCP traffic was supposed to pass through the Tofino™ SA between the safety system and the controllers, it was appropriate for the Tofino™ SA to block the multicast traffic. However, this generated numerous nuisance alarms, making it difficult for the system operator to respond to other alarms. To address this, a “Deny/No Log” rule was created to block this traffic, yet not report it as an alarm at the Tofino™ CMP.

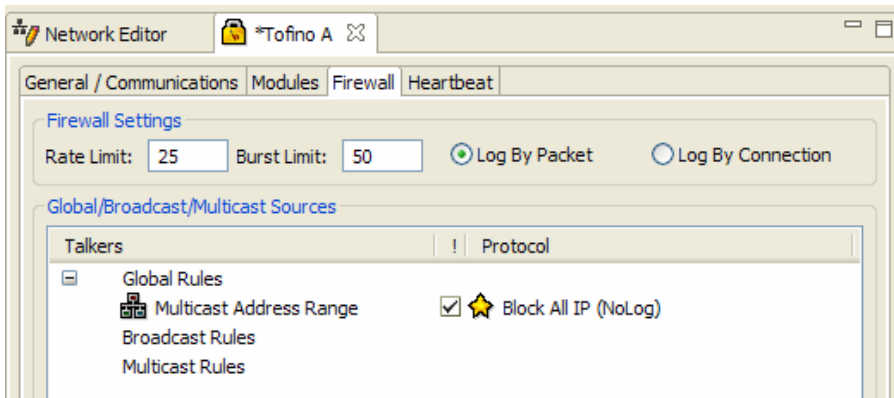


Figure 8: Addition of Special Rule to Block all IP Traffic from the “Multicast” Network

This involved creating a second Network node in the Tofino™ CMP Network Editor to represent all the multicast addresses noted in the alarm messages. Once this was in place, a ‘Block All IP – No Log’ special rule was selected from the Tofino™ Special Rule list and deployed as a rule on both Tofino™ SAs to block, but not report, any traffic directed to these multicast addresses. This ended all nuisance alarms from the multicast traffic on the network.

Conclusions

A half day was required to install and configure the Tofino™ Industrial Security Solution. The flexibility inherent in the Tofino™ CMP software made it simple to configure a network diagram in order to provide the necessary protection, while giving the operator an accurate view of the network traffic passing through the two Tofino™ Security Appliances. Test mode made firewall testing possible without impact to the operating process. Finally, this application indicates that Tofino™ SA works well in a redundant network installation and complements the security offered by the Honeywell™ Control System Firewalls and Cisco ASA firewall.

For additional information on Tofino™ SA installation, see **Tofino™ Installation Guide INM-9221**

For additional information on Tofino™ CMP configuration, see **Tofino™ CMP Help Manual**

Tofino™ is a registered trademark of Byres Security Inc. All other trademarks are acknowledged as the property of their respective owners.



EUROPE (EMEA)
AMERICAS
INTERNATIONAL
ASIA-PACIFIC

Tel: +44 (0)1582 723633
Tel: +1 888 9TOFINO
Tel: +1 780 485 3139
Tel: +65 6 487 7887

E-mail: tofinosupport@mtl-inst.com Web site: www.tofinosecurity.com



Mar 2008