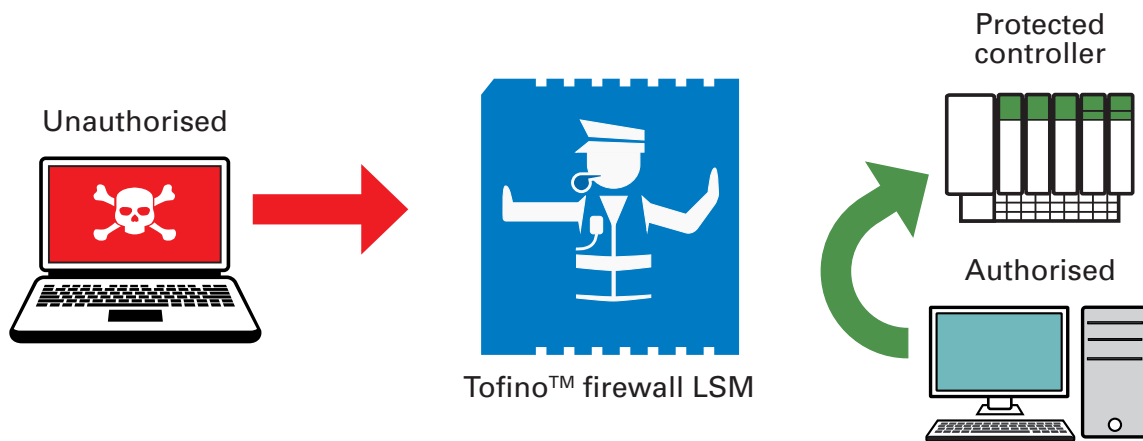


MTL Tofino™ firewall LSM

Directs and controls industrial network traffic



Take control of your network traffic

The vast majority of control networks have little or no isolation between different subsystems. If a device misconfiguration, hardware failure, or virus causes a problem in one part of the network, it can spread throughout the entire network in seconds and bring your whole plant down. Even redundant backup systems can fail simultaneously if their network connections are not protected.

The MTL Tofino Firewall LSM is like a traffic control cop for industrial networks, checking all communications on your control network against a list of traffic 'rules' defined by your control engineers. Any communication that is not on the 'allowed' list will be blocked and reported by the MTL Tofino Firewall. Traffic rules are created using terms and concepts that are already familiar to control specialists. And, the unique 'test' mode of MTL Tofino lets you test your rules without any risk to plant operation.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Improved system reliability and stability.

Unique capabilities:

- Traffic rules are defined by your control team, specifying which devices may communicate using what protocols.
- Rule definition is simple using a graphical drag-and-drop editor.
- Traffic that does not match the rules is automatically blocked and reported.
- Over 125 pre-defined IT and industrial communication protocols.
- Over 180 pre-defined security templates for common controllers, drives, HMIs and network products.
- Pre-defined 'special rules' for advanced traffic filtering and vulnerability protection.

Applications

- Isolate critical devices from threat sources.
- Separate control networks into security 'zones', restricting communications between zones.
- Protect controllers with known vulnerabilities.

FEATURES & SPECIFICATIONS

Protects multiple devices	Master and slave devices are supported, with unique direction and permission settings for each client/server connection.
Filter policy	Deny by default: any network traffic that is not on the 'allowed' list is automatically blocked and reported.
State tracking	Stateful Packet Inspection (SPI).
User-settable options	<p>IP-based protocols:</p> <ul style="list-style-type: none"> • Source device: specific IP address, network, or 'any'. • Destination device: specific IP address, network, broadcast, multicast, or 'any'. • Application protocol: any combination of single, list, and/or range of port numbers. • Direction: incoming, outgoing, bidirectional. <p>Both IP-based and non-IP protocols:</p> <ul style="list-style-type: none"> • Permission: Allow, Deny, Enforce (requires appropriate Enforcer LSM). • Logging: Enabled, Disabled. • Rate limit controls.
Transport protocols	TCP, UDP and non-IP protocols supported.
Configuration method	Simple configuration using the MTL Tofino Configurator (TC).
Operating modes	All standard MTL Tofino modes supported: <ul style="list-style-type: none"> • Passive: all traffic allowed, no alerting. • Test: all traffic allowed; alerts generated as per user rules. • Operational: traffic filtered and alerts generated as per user rules.
Security alerts	Reports blocked traffic to a syslog server and non-volatile memory on a MTL Tofino Security Appliance.
Certifications	<ul style="list-style-type: none"> • Certified Modbus compliant by Modbus-IDA.
System requirements	<ul style="list-style-type: none"> • MTL Tofino Security Appliance. • MTL Tofino Configurator (TC).
Ordering information	<p>Part number: 9522-FW Name: MTL Tofino™ Firewall LSM Visit: www.mtl-inst.com/tofino for ordering information for all products.</p>

The **MTL Tofino™ Firewall LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



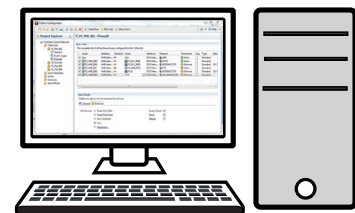
Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino SA:

- **Firewall:** Directs and controls industrial network traffic.
- **Modbus, OPC, and EtherNet/IP Enforcers:** Ensure compliance, manage connections, and restrict ICS SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino Configurator

Software that provides coordinated security management of all MTL Tofino Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2016 Eaton
All Rights Reserved
Publication No. EPS FW-LSM rev8 010916
September 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ Netconnect LSM

Secure remote configuration



Secure remote discovery, configuration, and verification of MTL Tofino devices.

The MTL Tofino Netconnect LSM lets the MTL Tofino Configurator and the MTL Tofino Security Appliance communicate securely over any network. This allows you to discover unconfigured MTL Tofino Security Appliances on the network, and apply and verify their configuration—all from your PC without having to physically visit the hardware devices in the field.

The Discovery feature lets you find the MTL Tofino Security Appliances on your network that were installed straight out of the box. Field technicians don't need to enter an IP address or set any dip switches. MTL Tofino Discovery works over any IP-based network, including wide area networks and routed LANs.

Once the configurations for a group of MTL Tofino Security Appliances are defined in the MTL Tofino Configurator, the NetConnect LSM lets you securely transfer those configurations to the devices in the field. The Verify command lets you record and verify the configuration of any MTL Tofino security Appliance, ensuring that the data in the hardware matches all information in the software database.

Saves you money through:

- Easy and reliable remote configuration of your MTL Tofino Security Appliances.
- Simple validation and auditing of all field configurations.
- Reduced maintenance and training costs for field installation of firewalls.

Unique capabilities:

- Stealthy IP address-free discovery and configuration over routed networks.
- Configuration and validation of multiple MTL Tofino Security Appliances.
- Simultaneous configuration and verification ensures system compliance.
- Automatic downloading of log and diagnostic files.
- Secure auditing of all changes to firewall configurations.

Typical applications

- Configuration of devices in remote locations, such as off-shore platforms and electrical substations.
- Configuration in sites where skilled security staff are unavailable.
- Compliance to standards like NERC CIP that require confirmation of firewall configurations in the field.

FEATURES & SPECIFICATIONS

Automatic discovery	Discover unconfigured MTL Tofino Security Appliances on any IP-based network, including networks with existing routers or firewalls.
Secure communication	<ul style="list-style-type: none"> • Uses secure SSH encryption technology to configure each MTL Tofino Security Appliance. • Unique keys generated for every MTL Tofino Security Appliance.
Multiple device configuration	Select one or many MTL Tofino Security Appliances to simultaneously apply the device configurations across a plant.
Verification	Remote verification of firmware versions and configurations, including version tracking and checksum validation.
Log and diagnostic file download	Remotely download event log and diagnostic files over the network.
Stealth addressing	Uses MTL Tofino's patented IP address-free communications technology.
Operating modes	All standard MTL Tofino modes supported: <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules. • Operational: traffic filtered and alerts generated as per user rules.
Upgrading firmware	Upload new firmware to MTL Tofino Security Appliances over the network.
Auditing	<ul style="list-style-type: none"> • Automatic auditing of user activity, including configuration changes to either the database or the in-field MTL Tofino Security Appliances. • All configurations signed to detect tampering or out of sync systems.
System requirements	<ul style="list-style-type: none"> • MTL Tofino security Appliance. • MTL Tofino Configurator. • MTL Tofino Firewall/Event Logger LSM.
Ordering information	Part number: 9522-NET Name: MTL Tofino™ Netconnect LSM Visit: www.mtl-inst.com/tofino for ordering info for all products.

The **MTL Tofino™ Netconnect LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



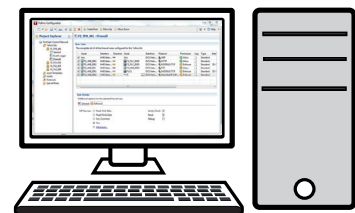
Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino SA:

- **Firewall:** Directs and controls industrial network traffic.
- **Modbus, OPC, and EtherNet/IP Enforcers:** Ensure compliance, manage connections, and restrict ICS SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino Configurator

Software that provides coordinated security management of all MTL Tofino Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2016 Eaton
All Rights Reserved
Publication No. EPS NC-LSM rev2 010916
September 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

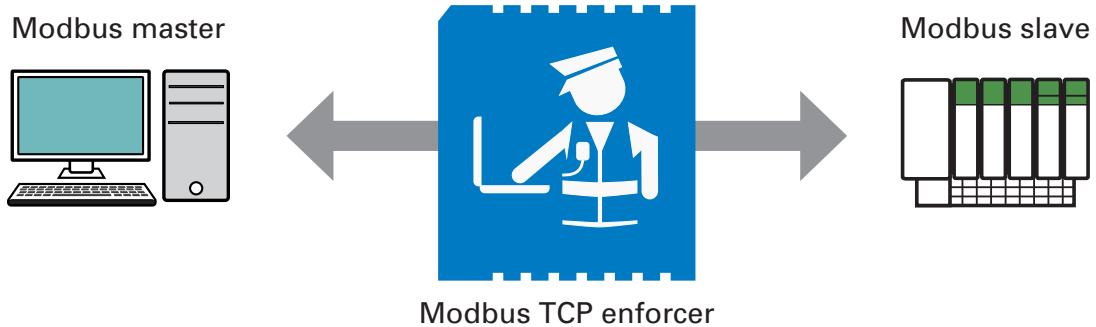
THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ modbus TCP enforcer LSM

Content Inspection for Modbus



Advanced cyber threat and safety protection for your Modbus devices

Did you know that any device with a network connection to a Modbus controller can potentially CHANGE any of the controller's I/O points or register values? Many controllers can even be reset, disabled, or loaded with new logic or firmware.

The MTL Tofino Modbus TCP Enforcer is a content inspector for Modbus communications, checking every Modbus command and response against a list of 'allowed' commands defined by your control engineers. Any command that is not on the 'allowed' list, or any attempt to access a register or coil that is outside the allowed range, is blocked and reported.

The MTL Tofino Modbus TCP Enforcer makes sure that the only Modbus commands your control devices receive are approved commands from approved computers. Accidents involving remote programming are prevented and corrupted messages are blocked, making your control system safer and more reliable.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.
- Improved system reliability and stability.

Unique capabilities:

- First-ever application of content inspection technology to industrial protocols.
- Control specialist defines list of allowed Modbus commands, registers and coils.
- Automatically blocks and reports any traffic that does not match the rules.
- Protocol 'Sanity Check' blocks any traffic not conforming to the Modbus standard.
- Supports multiple master and slave devices.
- Simple configuration and monitoring using the MTL Tofino Configurator GUI.
- Certified Modbus compliant by Modbus-IDA.

Applications

- Oil & gas custody transfer.
- Safety instrumentation systems.
- Managing PLC programming stations.
- Display-only HMI panels.
- Partner access to telemetry data.

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple master and slave Modbus devices are supported, with a unique set of inspection rules and options for each master/slave connection.
Default filter policy	Deny by default: any network traffic that is not on the 'allowed' list is automatically blocked and reported.
Modbus function codes	Supports functions 1-8, 11-17, 20-24, 40, 42, 43, 48, 66, 67, 91, 100, 125, 126.
User-settable options	The following options may be set on a per-connection basis: <ul style="list-style-type: none"> • Permitted Modbus function codes. • Permitted register or coil address range. • Permitted Modbus Unit IDs. • Sanity check enable/disable. • State tracking enable/disable. • TCP Reset on blocked traffic (when utilizing TCP transport protocol). • Modbus exception reply on blocked traffic.
Transport protocols	Both Modbus/TCP and Modbus/UDP supported.
Configuration method	Simple configuration using the MTL Tofino Configurator (TC).
Throughput	1000 packets per second with full content inspection.
Operating modes	All standard MTL Tofino modes supported: <ul style="list-style-type: none"> • Passive: all traffic allowed, no alerting. • Test: all traffic allowed; alerts generated as per user rules. • Operational: traffic filtered and alerts generated as per user rules.
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino Security Appliance.
Certifications	Certified Modbus compliant by Modbus-IDA.
System requirements	<ul style="list-style-type: none"> • MTL Tofino Security Appliance. • MTL Tofino Firewall LSM. • MTL Tofino Configurator (TC).
Ordering information	Part number: 9522-MBT Name: MTL Tofino™ Modbus TCP Enforcer LSM Visit: www.mtl-inst.com/tofino for ordering info for all products.

The **MTL Tofino™ Firewall LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



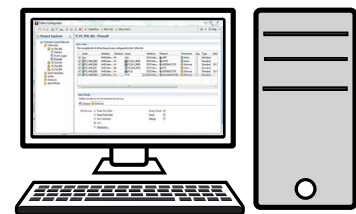
Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino SA:

- **Firewall:** Directs and controls industrial network traffic.
- **Modbus, OPC, and EtherNet/IP Enforcers:** Ensure compliance, manage connections, and restrict ICS SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino Configurator

Software that provides coordinated security management of all MTL Tofino Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2016 Eaton
All Rights Reserved
Publication No. EPS MBT-LSM rev6 10916
September 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

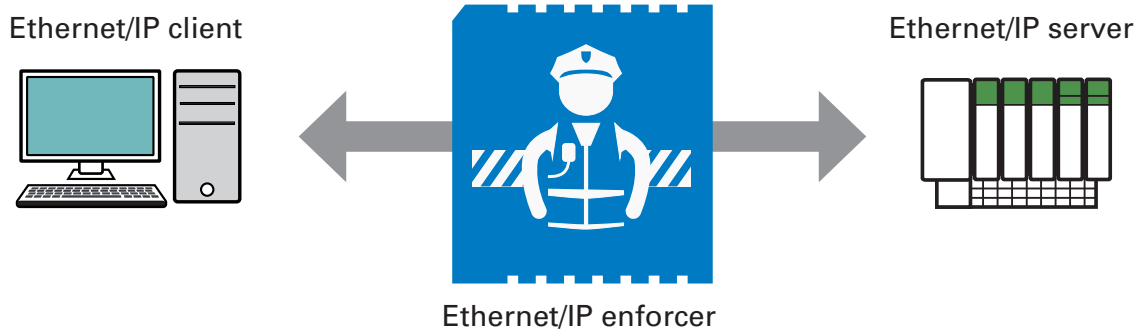
THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ ethernet/IP enforcer LSM

Content inspection for ethernet/IP



Advanced cyber threat and safety protection for your EtherNet/IP devices

EtherNet/IP and CIP are excellent protocols for managing Industrial Control Systems (ICS). Unfortunately, they were never designed with security in mind. If an individual is allowed to read data from a controller, then chances are they can also shut down or reprogram the controller.

The MTL Tofino EtherNet/IP Enforcer Loadable security Module (LSM) is a content inspector for EtherNet/IP communications, checking every message against a list of 'allowed' objects and services. You can choose from pre-defined lists of common actions, such as Read-Only, or you can build your own custom list of objects and services. Any service that is not on the 'allowed' list, or any attempt to access an object that is not approved, is blocked and reported.

The MTL Tofino EtherNet/IP Enforcer LSM makes sure that the only messages your control devices receive are approved commands from approved computers. Accidents involving remote programming are prevented and corrupted messages are blocked, making your control system safer and more reliable.

Saves you money through:

- Improved system reliability and stability.
- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.

Unique capabilities:

- Simple configuration using the MTL Tofino configurator's graphical user interface.
- One-click setup for secure 'read-only' communications to controllers.
- Protocol 'Sanity Check' blocks any traffic not conforming to the ODVA standards.
- Supports multiple EtherNet/IP clients and servers.
- Control specialists can optionally define lists of allowed CIP objects and services.
- Automatically blocks and reports any traffic that does not match the rules.
- Secures all EtherNet/IP CIP Class 3 Explicit messaging.

Typical applications

- Mission critical automation systems.
- Protecting safety instrumentation systems.
- Managing PLC programming stations.
- Display-only HMI panels.
- Secure remote access to PLC data.

MTL Tofino™ ethernet/IP enforcer LSM

February 2017

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple client and server EtherNet/IP devices are supported with a unique set of inspection rules and options for each client/server connection.
Default filter policy	Deny by default: any CIP object or service that is not on the 'allowed' list is automatically blocked and reported.
User-settable options	The following options may be set on a per-connection basis: <ul style="list-style-type: none"> • Permitted message type (Read-Only Data, Read/Write Data, Any, Advanced). • Permitted CIP object class. • Permitted CIP service for each class. • Custom or vendor-specific objects and services. • Sanity check enable/disable. • TCP Reset on blocked traffic. • EtherNet/IP debug reply on blocked traffic.
Supported message types	All CIP class 3 explicit messages.
Configuration method	Simple configuration using the MTL Tofino configurator.
Throughput	1000 packets per second with full content inspection.
Operating modes	All standard MTL Tofino modes supported: <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules. • Operational: traffic filtered and alerts generated as per user rules.
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino Security Appliance.
Tested equipment	Tested for use with all Rockwell ControlLogix and Schneider PLCs.
System requirements	<ul style="list-style-type: none"> • MTL Tofino Security Appliance. • MTL Tofino Firewall/Event Logger LSM. • MTL Tofino Configurator.
Ordering information	Part number: 9522-EIP Name: MTL Tofino™ EtherNet/IP Enforcer LSM For additional information visit: www.mtl-inst.com/tofino for ordering info for all products

The **MTL Tofino™ EtherNet/IP Enforcer LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



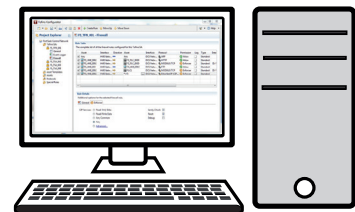
Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino SA:

- **Firewall:** Directs and controls industrial network traffic.
- **Modbus, OPC, and EtherNet/IP Enforcers:** Ensure compliance, manage connections, and restrict ICS SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino configurator

Software that provides coordinated security management of all MTL Tofino Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2017 Eaton
All Rights Reserved
Publication No. EPS EIP-LSM rev3 080217
February 2017

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ OPC enforcer LSM

Tracks and secures OPC connections



Advanced cyber security for OPC/DCOM Communications.

OLE for Process Control (OPC) is widely used in SCADA and control systems as an interoperability solution, interfacing control applications from multiple vendors. But the DCOM technologies underlying OPC were designed before network security issues were widely understood. As a result, OPC is almost impossible to secure using a conventional firewall.

The MTL Tofino OPC Enforcer Loadable Security Module (LSM) inspects, tracks and secures every connection that is created by an OPC application. It dynamically opens only the TCP ports that are required for each connection, and only between the specific OPC client and server that created the connection.

It's simple to use – no configuration changes are required on the OPC clients and servers – and offers superior security over what can be achieved with conventional firewall or tunneler solutions.

Your OPC clients and servers are vital to the operation of your plant. Protect them now with the MTL Tofino Security Appliance and MTL Tofino OPC Enforcer LSM.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.
- Improved system reliability and stability.

Unique capabilities:

- First-ever application of content inspection technology to industrial protocols.
- Control specialist defines list of allowed Modbus commands, registers and coils.
- Automatically blocks and reports any traffic that does not match the rules.
- Protocol 'Sanity Check' blocks any traffic not conforming to the Modbus standard.
- Supports multiple master and slave devices.
- Simple configuration and monitoring using the MTL Tofino Configurator GUI.
- Certified Modbus compliant by Modbus-IDA.

Applications

- Oil & gas custody transfer.
- Safety instrumentation systems.
- Managing PLC programming stations.
- Display-only HMI panels.
- Partner access to telemetry data.

FEATURES & SPECIFICATIONS

Supports all variations of DCOM-based OPC	Data Access (DA), Historical Data Access (HDA), Alarms and Events (A&E), Data eXchange (DX), and XML Data Access (XML-DA).
Supports multiple connections	Multiple OPC clients and servers can be protected by a single MTL Tofino Security Appliance running the OPC Enforcer LSM.
Default filter policy	Deny by default including: <ul style="list-style-type: none"> • Any attempted OPC traffic that is not between defined OPC client and server pairs will be blocked and reported. • Any attempted TCP connection that was not successfully negotiated between a valid OCP client and server will be blocked and reported.
User-settable options	The following options may be set: <ul style="list-style-type: none"> • Sanity check enable/disable. • Packet fragmentation controls. • Maximum time to wait for data connection to start.
Configuration method	Simple configuration using the MTL Tofino Configurator (TC).
Operating modes	All standard MTL Tofino modes supported: <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules. • Operational: traffic filtered and alerts generated as per user rules.
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino Security Appliance.
Certifications	Certified Modbus compliant by Modbus-IDA.
System requirements	<ul style="list-style-type: none"> • MTL Tofino Security Appliance. • MTL Tofino Firewall LSM. • MTL Tofino Configurator (TC).
Ordering information	Part number: 9522-OPC Name: MTL Tofino™ OPC Enforcer LSM Visit: www.mtl-inst.com/tofino for ordering info for all products.

The **MTL Tofino™ Firewall LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



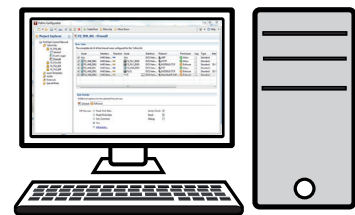
Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino SA:

- **Firewall:** Directs and controls industrial network traffic.
- **Modbus, OPC, and EtherNet/IP Enforcers:** Ensure compliance, manage connections, and restrict ICS SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino Configurator

Software that provides coordinated security management of all MTL Tofino Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2016 Eaton
All Rights Reserved
Publication No. EPS OPC-LSM rev 3 010916
September 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ DNP3 Enforcer LSM

A plug-in Deep Packet Inspection (DPI) module that provides real-time validity checking and content inspection for DNP3 traffic.



The MTL Tofino™ DNP3 Enforcer Loadable Security Module (LSM) is a plug-in Deep Packet Inspection (DPI) module providing Advanced Cyber Threat and Vulnerability Protection for DNP3 Protocol Communications making sure that the only DNP3 commands your control devices receive are approved commands from authorized computers.

Distributed Network Protocol (DNP3) is IEEE Standard for Electric Power Systems Communications. It's the popular, open utility protocol that emphasizes reliability and less bandwidth usage.

While widely used in power and utility networks, DNP3 also face security vulnerabilities, not only on the slave device, but the master stations as well. Successfully attack a PLC or RTU in a substation and you might knock that station off line. Successfully attack a SCADA master and you can knock a whole system off line.

The MTL Tofino™ DNP3 Enforcer LSM enables deep packet inspection (DPI) capabilities for DNP3 traffic. It ensures that end values are greater than the starting values. If this isn't the case, the Tofino security appliance should drop the packet REGARDLESS of data content. Thus no matter what the attacker puts in his/her payload, or how he/she tried to obfuscate it with techniques like NOP slides, the checks will detect and block the attack. The installation engineer can specify master/slave device pairs between which DNP3 traffic will be allowed to flow. Only correctly formatted DNP3 traffic will be allowed.

DNP3 validation includes checking of common header byte fields, packet lengths, and DNP3 CRC values.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.
- Improved system reliability and stability.

Unique capabilities:

- Unique deep packet inspection technology for industrial protocols
- Control specialist defines list of allowed DNP3 message type and function codes
- Automatically blocks and reports any traffic that does not match the rules
- Protocol 'Sanity Check' blocks any traffic not conforming to the DNP3 standard
- Supports multiple master and slave devices
- Simple configuration using the Tofino Configurator's graphical user interface

Applications

- SCADA Master Station protection
- Cyber security solution for PLCs, RTUs, IEDs, DCS
- NERC-CIP Compliance
- Electric utility transmission and transmission substation security
- Prevents malware and Man-in-the-Middle attacks

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple master and slave DNP3 devices are supported with a unique set of inspection rules and options for each master/slave connection
Default filter policy	Deny by default: any DNP3 function code that is not on the 'allowed' list is automatically blocked and reported
User-settable options	The following options may be set on a per-connection basis: <ul style="list-style-type: none"> • Permitted DNP3 function codes • Check outstation traffic • Permitted DNP3 Unit IDs • Sanity check enable/disable • CRC check • TCP Reset on blocked traffic (when utilizing TCP transport protocol) • DNP3 exception reply on blocked traffic
Configuration method	Simple configuration using the MTL Tofino™ Configurator (TC).
Throughput	2000 packets per second with full content inspection
Operating modes	All standard Tofino modes supported: <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules • Operational: traffic filtered and alerts generated as per user rules
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino™ Security Appliance.
Certifications	Certified Modbus compliant by Modbus-IDA.
System requirements	<ul style="list-style-type: none"> • MTL Tofino™ (9202-ETS) Industrial Security Appliance. These new enforcers cannot be run in older systems. They will work for existing MTL Tofino™ (9202-ETS) in the field • MTL Tofino™ Firewall/Event Logger LSM • MTL Tofino™ Configurator
Ordering information	Part number: 9522-DNP3 Name: MTL Tofino™ DNP3 Enforcer LSM Visit: www.mtl-inst.com/product/9202-ets_mtl_tofino_network_security_solution/

The **MTL Tofino™ DNP3 Enforcer LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino™ Industrial Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino™ SA:

- **Firewall:** Monitors and controls industrial network traffic.
- **Modbus, OPC, EtherNet/IP, DNP3, IEC 104 and GOOSE Enforcers:** Ensure compliance, manage connections, and restrict ICS/ SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino™ Configurator (3.2)

Software that provides coordinated security management of all MTL Tofino™ Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2018 MTL
All Rights Reserved
Publication No. EPS DNP3-LSM rev 1 090218
February 2018

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ IEC-104 Enforcer LSM

A plug-in Deep Packet Inspection (DPI) module that provides real-time validity checking and content inspection for IEC 60870-5-104 traffic.



The MTL Tofino™ IEC 104 Enforcer LSM makes sure that the only IEC 104 commands your control devices receive are approved commands from approved computers.

IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for Supervisory Control and Data Acquisition (SCADA) in electrical engineering and power system automation applications. IEC 60870- 5-104 (IEC 104) Transmission Protocol is the companion standard that suits the complete network access. IEC 60870-5-104 is a de facto industry standard protocol for implementing parts of SCADA communications. The protocol enables the Master Station to request data from Substations using pre-defined commands and Substations to respond by transmitting the requested data.

As IEC 60870-5-104 was not designed with security mechanisms in mind. The protocol itself lacks any form of authentication or encryption. With increased Internet connectivity by industrial control systems, the protocol can be susceptible to conventional TCP/IP-based attacks that could compromise or negatively affect operations.

MTL Tofino™ IEC 104 Enforcer LSM enables DPI capabilities for IEC 104 traffic. The installation engineer specifies master station (client) /substation (server) device pairs between which IEC 104 traffic will be allowed to flow. MTL Tofino™ Configurator (TC) provides users with the capability of specifying various IEC 104 application layer parameter options and formatting. Only correctly formatted IEC 104 packets will be allowed.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.
- Improved system reliability and stability.

Unique capabilities:

- Unique deep packet inspection technology for industrial protocols
- Control specialist defines list of allowed IEC 104 message type and function codes
- Automatically blocks and reports any traffic that does not match the rules
- Protocol 'Sanity Check' blocks any traffic not conforming to the IEC 104 standard
- Supports multiple master and slave devices
- Simple configuration using the Tofino Configurator's graphical user interface

Applications

- SCADA network protection
- Prevent Man-in-the-Middle attacks
- Mission-critical Control Systems
- Electric utility transmission and transmission substation security
- Cybersecurity solution for PLCs, RTUs, IEDs, DCS, and others

MTL Tofino™ IEC-104 Enforcer LSM

February 2018

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple master and slave IEC 104 devices are supported with a unique set of inspection rules and options for each master/slave connection
Default filter policy	Deny by default: any IEC 104 function code that is not on the 'allowed' list is automatically blocked and reported
User-settable options	<p>The following options may be set on a per-connection basis:</p> <ul style="list-style-type: none"> • Permitted common address and I/O address size • Permitted originator address and common address • Permitted IEC 104 Unit IDs • Sanity check enable/disable • TCP Reset on blocked traffic (when utilizing TCP transport protocol) • Cause of Transmission Size (COT)
Configuration method	Simple configuration using the MTL Tofino™ Configurator (TC).
Throughput	2000 packets per second with full content inspection
Operating modes	<p>All standard Tofino modes supported:</p> <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules • Operational: traffic filtered and alerts generated as per user rules
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino™ Security Appliance.
Certifications	Certified Modbus compliant by Modbus-IDA.
System requirements	<ul style="list-style-type: none"> • MTL Tofino™ (9202-ETS) Industrial Security Appliance. These new enforcers cannot be run in older systems. They will work for existing MTL Tofino™ (9202-ETS) in the field • MTL Tofino™ Firewall/Event Logger LSM • MTL Tofino™ Configurator
Ordering information	<p>Part number: 9522-IEC104 Name: MTL Tofino™ IEC 104 Enforcer LSM Visit: www.mtl-inst.com/product/9202-ets_mtl_tofino_network_security_solution/</p>

The **MTL Tofino™ IEC 104 Enforcer LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino™ Industrial Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino™ SA:

- **Firewall:** Monitors and controls industrial network traffic.
- **Modbus, OPC, EtherNet/IP, DNP3, IEC 104 and GOOSE Enforcers:** Ensure compliance, manage connections, and restrict ICS/ SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino™ Configurator (3.2)

Software that provides coordinated security management of all MTL Tofino™ Security Appliances from one workstation or server.



Eaton Electric Limited,
 Great Marlings, Butterfield, Luton
 Beds, LU2 8DL, UK.
 Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
 E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2018 MTL
 All Rights Reserved
 Publication No. EPS IEC-104-LSM rev 1 090218
 February 2018

EUROPE (EMEA):
 +44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
 +1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
 +65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.

MTL Tofino™ GOOSE Enforcer LSM

A plug-in Deep Packet Inspection (DPI) Module that provides real-time validity checking and content inspection for GOOSE traffic.



The MTL Tofino™ Generic Object-Oriented System Events (GOOSE) Enforcer module provides real-time validity checking and content inspection for GOOSE traffic, ensuring your control devices receive only approved commands from authorized sources.

Benefits:

As industrial networks and devices become more connected to external networks, the potential to expose GOOSE messages and IEC 61850 traffic – a global standard for communication networks and systems within substations – to outside intruders increases exponentially.

The MTL Tofino™ GOOSE Enforcer LSM enables DPI capabilities for GOOSE traffic. The enforcer applies multiple security standards and defensive layers to GOOSE messages, including authentication of data transfers through digital protocol validation, prevention of eavesdropping and spoofing and intrusion detection.

These defensive protocols protect networks against harmful attacks, such as ARP, MAC flooding, spanning-tree, multicast brute force and other VLAN-related attacks. The strict latency requirements (sending real-time data transmissions between devices within 4 ms) and DPI capabilities prevent any malicious, malformed or out-of-sequence packet to pass through protected networks.

Applications:

With many new capabilities, the MTL Tofino™ GOOSE Enforcer LSM is best suited for sectors that require enhanced DPI to prevent malware and Man-in-the-Middle attacks, as well as ones that support large network communication, SCADA Master Station protection and NERC CIP compliance. With improved time-saving features, seamless integration onto existing networks and enhanced security, the solution is ideal for networks that rely on long-distance communication between sending and receiving devices, such as substations and control centers.

Markets:

The MTL Tofino™ GOOSE Enforcer LSM is designed to protect equipment and systems that use GOOSE messaging, and in particular substation automation and other utility applications. The MTL Tofino™ GOOSE Enforcer LSM can be used in conjunction with other MTL Tofino™ Enforcers to provide comprehensive protection for a wide range of industrial protocols and devices and to span other applications including the transportation, manufacturing, machine building, food and beverage, and water/wastewater markets.

Saves you money through:

- Simplifying compliance to safety and security standards with superior protection against attacks and misconfigurations.
- Reduced down time and production losses by managing large deployments of data from a central location.

Unique capabilities:

- Delivers unique DPI technology for all protocols
- Enables control specialist to define a list of allowed GOOSE PDU parameters such as sequence numbers and stream numbers
- Automatically blocks and reports any traffic that does not match established rules
- Performs protocol 'sanity check' to block any GOOSE traffic not conforming to the standard
- Supports multiple master and slave devices
- Leverages new syslog view for holistic network security and simplified maintenance
- The MTL Tofino™ GOOSE Enforcer LSM offers advanced security features and simplified integration capabilities to bring efficiency and reliability to large-scale deployments, especially in energy and utility markets.

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple master and slave GOOSE devices are supported with a unique set of inspection rules and options for each master/slave connection.
Default filter policy	Deny by default: any GOOSE Frame with destination MAC address not in the broadcast or multicast range is automatically blocked and reported. Also all GOOSE Frames with source MAC address that is not on the 'allowed' list are automatically blocked and reported.
User-settable options	The following options may be set on a per-connection basis: <ul style="list-style-type: none"> • Enable sanity check on PDU data length and field value. • Enable system to check if the packet source is remote otherwise the Enforcer treats the packet to be local for deep packet inspection. • Enable a sequence check on incoming PDU packets with the same application id.
Configuration method	Simple configuration using the MTL Tofino™ Configurator (TC).
Throughput	2000 packets per second with full content inspection
Operating modes	All standard Tofino modes supported: <ul style="list-style-type: none"> • Test: all traffic allowed; alerts generated as per user rules • Operational: traffic filtered and alerts generated as per user rules
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino™ Security Appliance.
System requirements	<ul style="list-style-type: none"> • MTL Tofino™ (9202-ETS) Industrial Security Appliance. These new enforcers cannot be run in older systems. They will work for existing MTL Tofino™ (9202-ETS) in the field • MTL Tofino™ Firewall/Event Logger LSM • MTL Tofino™ Configurator VERSION 3.2
Ordering information	Part number: 9522-GOOSE Name: MTL Tofino™ GOOSE Enforcer LSM Visit: www.mtl-inst.com/product/9202-ets_mtl_tofino_network_security_solution/

The **MTL Tofino™ GOOSE Enforcer LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino™ Industrial Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.



Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino™ SA:

- **Firewall:** Monitors and controls industrial network traffic.
- **Modbus, OPC, EtherNet/IP, DNP3, IEC 104 and GOOSE Enforcers:** Ensure compliance, manage connections, and restrict ICS/ SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino™ Configurator (3.2)

Software that provides coordinated security management of all MTL Tofino™ Security Appliances from one workstation or server.



Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2018 MTL
All Rights Reserved
Publication No. EPS GOOSE-LSM rev 1 090218
February 2018

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.