FUTURE FIBRE
TECHNOLOGIES

NETWORK INFRASTRUCTURE PROTECTION

FFT SOLUTIONS

FFT's range of network physical security solutions employ laser based fiber optic sensing technologies to detect unauthorized cable access, data tapping, tampering and cable theft.

From desktop LANs to countrywide backbone networks, FFT offers solutions that pinpoint physical intrusions and provide actionable alarms that enable network administrators to isolate the problem, reroute network traffic and respond to the threat.

Applications

- Military Classified Networks
- Telecom Pathways
- Metro Fiber Rings
- Manholes and Telecom Vaults
- Aerial Fiber Networks
- Data Center LANs
- Industrial Control Networks

THE THREAT TO ENTERPRISE NETWORKS

Cyber security has traditionally focused on protecting customer databases and other IT assets using firewalls, encryption, and virus detection. These internet-facing solutions fall short when it comes to the enterprise network infrastructure, which can often extend beyond an organization's premises.

The distributed nature of enterprise networks combined with their accessibility make them one of the most vulnerable operational resources within any organization. For manufacturers, utilities, and energy companies, industrial networks are integral to the company's daily operation and present an even more critical risk than the corporate IT network.

Some of the most serious emerging cyber threats involve criminals taking control of military, industrial, and corporate networks to steal critical information, disrupt operations, and even destroy critical infrastructure. Organizations have been compromised by data tapped off the network, or disruption of services due to severed data links, and even simple cable theft.

This new threat requires a higher level of security to ensure that IT resources and critical communications are protected. Ongoing developments in code-breaking software prove that encryption alone is no longer sufficient to ensure that enterprise data is protected. For years, sophisticated military networks have combined encryption with physical infrastructure security. Hardening the enterprise network infrastructure is an essential security component for protection against today's cyber threats.

Networks at Risk

- Local Area
- Metro Area
- Wide Area
- Point-to-Point

Industries

- Military
- Government
- Telecom
- Utilities
- Oil/Gas
- Financial
- Manufacturing
- Healthcare

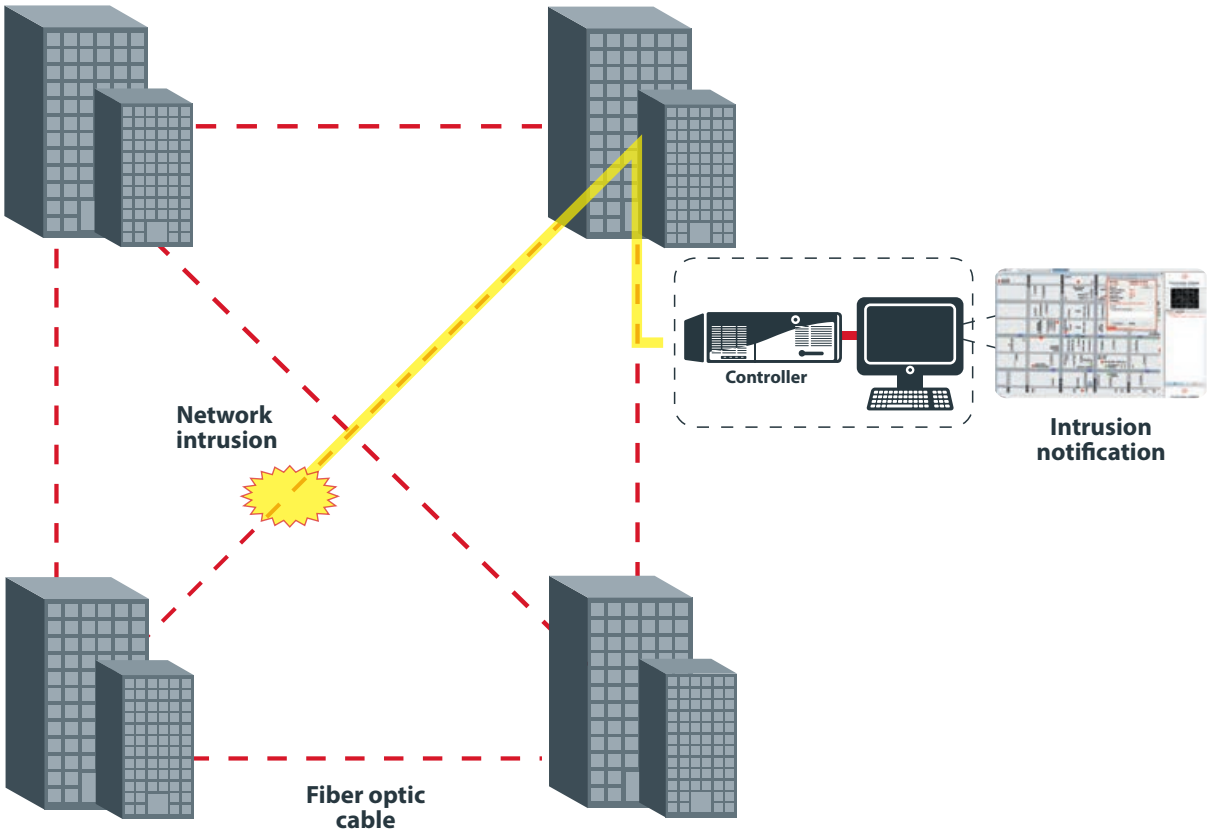
FFT SOLUTIONS

FFT's network physical security solutions ensure any portion of enterprise, operational, or industrial networks can be monitored in real time to automatically detect suspicious or unauthorized physical damage or access to network infrastructure.

Using sophisticated fiber optic signal analysis techniques, FFT systems operate in parallel with the operational network using standard fiber optic sensing cables. FFT systems reliably detect physical attempts to access the network and precise location of the event is provided in real time so network segments can be isolated and communications traffic re-routed.

FFT's approach has the added benefit of operating outside the communications network so monitoring does not impact network performance (like encryption can) A continuous fiber optic sensor creates an intelligent security blanket that overlays the critical network. Spare fiber optic strands can often be used to create a quickly deployed and comprehensive intrusion detection system.

FFT solutions are available to protect and monitor short network segments, network access via manholes, country-wide telecom deployments and even co-located copper cable. High-end FFT solutions locate intrusions to within six meters and can even detect nearby activity such as excavation, tunneling, manual digging, and vehicles.



A CONSISTENT APPROACH

Simple to install and operate, all of FFT solutions feature a sensing controller that combines a high performance fiber optic laser with a suite of hardware and software designed for capture and analysis of the returned light signal.

At the heart of the system is the intelligence built into the sensing controller. A laser beam is transmitted along the fiber optic cable used as a sensor in parallel with the communications segment being monitored. The returned signal is constantly monitored and analyzed for disturbances. Actual intrusion events are processed and forwarded to the FFT CAMS management system for alarm notification and presentation at the operator's console.

When FFT CAMS receives an intrusion event, the incident is filtered based on site-specific protocols. If the intrusion alarm is valid, then the area or zone where the alarm was triggered along with GPS coordinates are instantly displayed on the customer's site map, and the event is automatically logged into a secure database.

The alarm data can be forwarded via TCP/IP to external command and control or network management applications via SNMP traps or SDK integration with FFT CAMS.

FFT DESIGN BENEFITS

Near zero maintenance
- Low cost of ownership

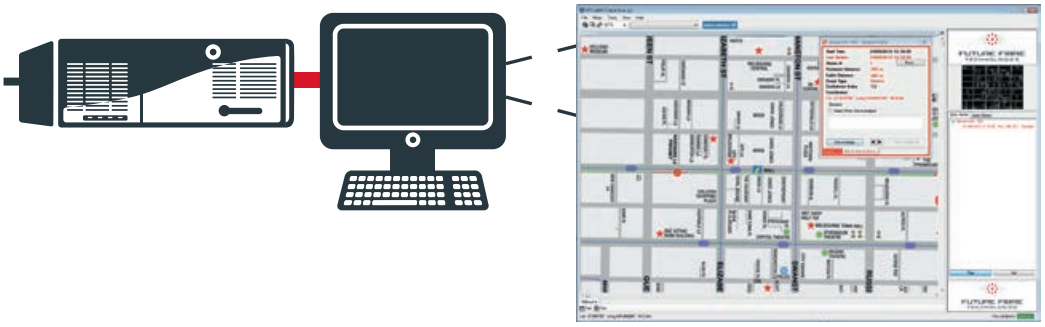
Use existing dark fiber optic strands
- Low acquisition costs

Centralize controllers in secure facility
- Reduce risk

Single management app across all solutions
- Low operations costs

FROM DETECTION TO LOCATION

(1) FFT Controller
(emits and receives laser light, real time signal analysis)

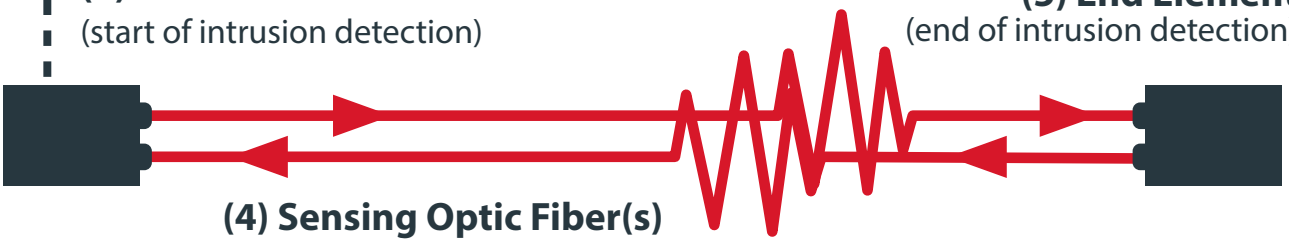


(6) FFT CAMS Software
(displays intrusion type and location)

(2) Fiber optic Lead-in Cable
(insensitive, transmits laser light)

(3) Start Element
(start of intrusion detection)

(5) End Element
(end of intrusion detection)



(4) Sensing Optic Fiber(s)
(detects distubance due to intrusion)

SECURE LINK

FFT Secure Link

Secure Link is a high-performance distributed fiber optic sensing system that has been deployed by financial institutions, telecom providers, government agencies, and the US Military for over a decade.

Secure Link complies with the NSTISSI-7003- compliant Armed Carrier PDS solution from NIS and has been used for critical network protection around the world.

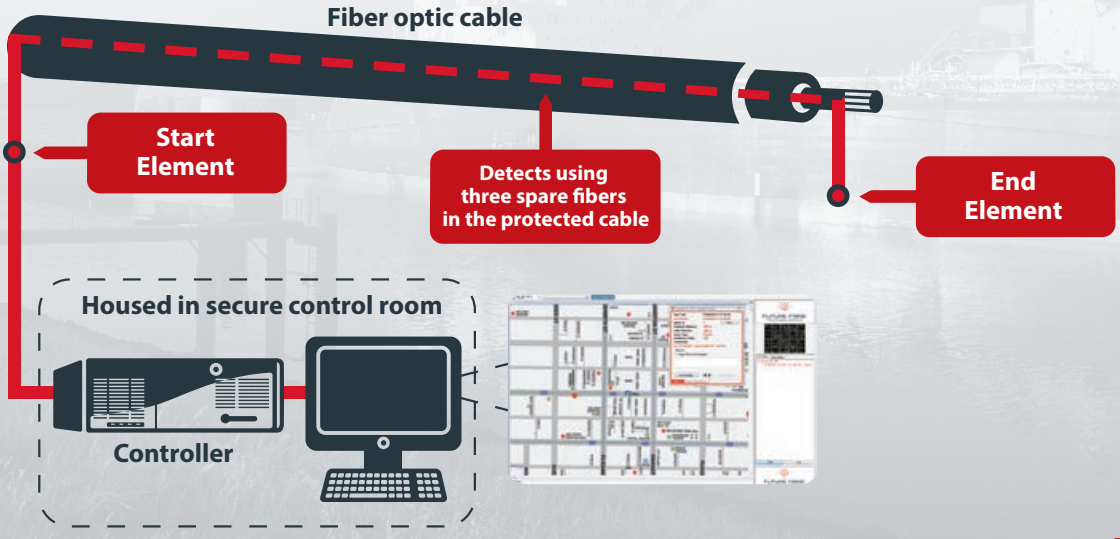
Like all FFT network solutions, Secure Link operates in parallel to the operational network. There is no impact to network performance and the Secure Link system cannot be used as a means of accessing the customer's network. In effect, Secure Link provides an "air gap" to physically isolate the intrusion detection system from the secure network.

Secure Link's sophisticated signal analysis techniques ensure reliable non-stop detection 24/7 year round. Secure Link reports the location of a network intrusion to within 25 meters (82 ft). Network intrusions include penetration of the conduit or duct bank, handling of adjacent cables, cutting or stripping cables, attaching tapping devices to the cable.

Applications include campus backbones, point-to-point network segments, metro networks, and city fiber rings.

FEATURES

- Single controller supports sensing for up to 40km (25 miles)
- Software zones can be easily changed to fit customer needs
- Locates intrusions to within 25 meters (82 ft) along the sensor
- Detects cable handling within a conduit and tampering with the conduit
- Proven technology deployed by international governments and US military



SECURE POINT

FFT Secure Point

Secure Point is a dual zone fiber optic sensing system that features two independent hardware zones, each of which can be up to 1.6km (1 mile) in length. Multiple Secure Point controllers can be combined to create a single sensor that supports up to 64 detection zones.

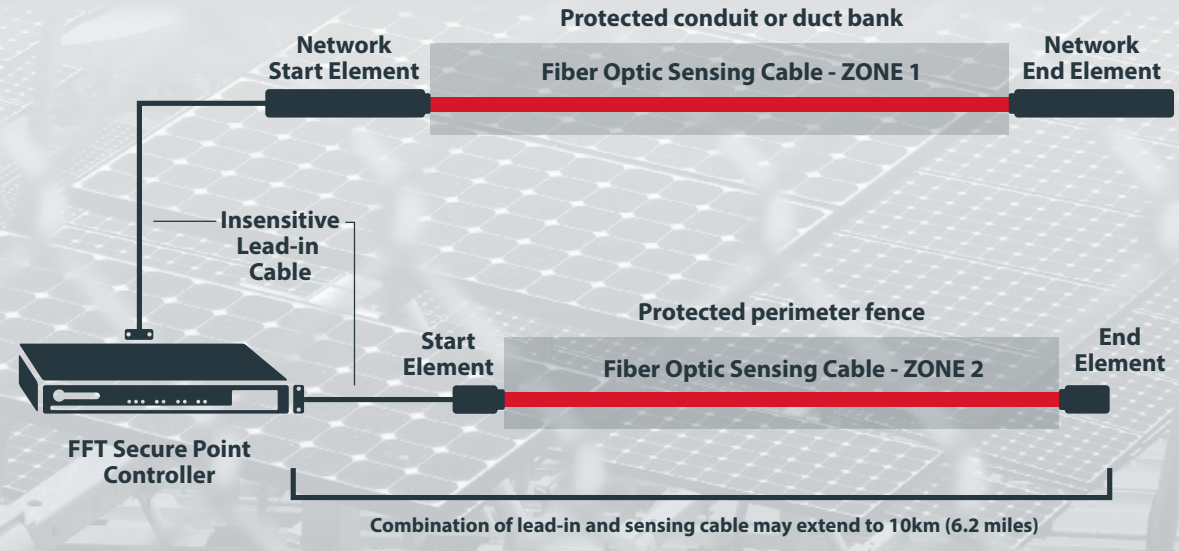
Designed with affordability in mind, the rugged Secure Point controller also features FFT's high performance detection and classification algorithms typically found only in very high-end systems. This ensures highly reliable intrusion detection even in extreme weather and climates ranging from tropical to arctic conditions.

With two independent detection zones, Secure Point can be used as a dual purpose solution for unmanned sites such as utility substations, solar farms, pumping stations, and water treatment facilities. One zone can monitor a critical network segment while the other zone simultaneously detects intruders cutting or climbing the perimeter fence.

With a lead in cable of upto 10km (6.2 miles), the Secure Point controller can be located some distance from the two detection zones and the asset to be monitored. This allows the electronic controllers to be housed in a secure facility with insensitive fiber optic cable leading out to the critical network segment. This feature dramatically simplifies the solution design by eliminating the need for power along the pathway.

FEATURES

- Single controller supports two sensing zones
- Stack controllers to create up to 64 zones
- Simple installation combined with powerful detection
- Monitors workgroup LANs, collapsed backbones, and point-to-point links
- Ideal for unmanned facilities that require both network security and perimeter intrusion detection



AURA

FFT Aura SR FFT Aura LR

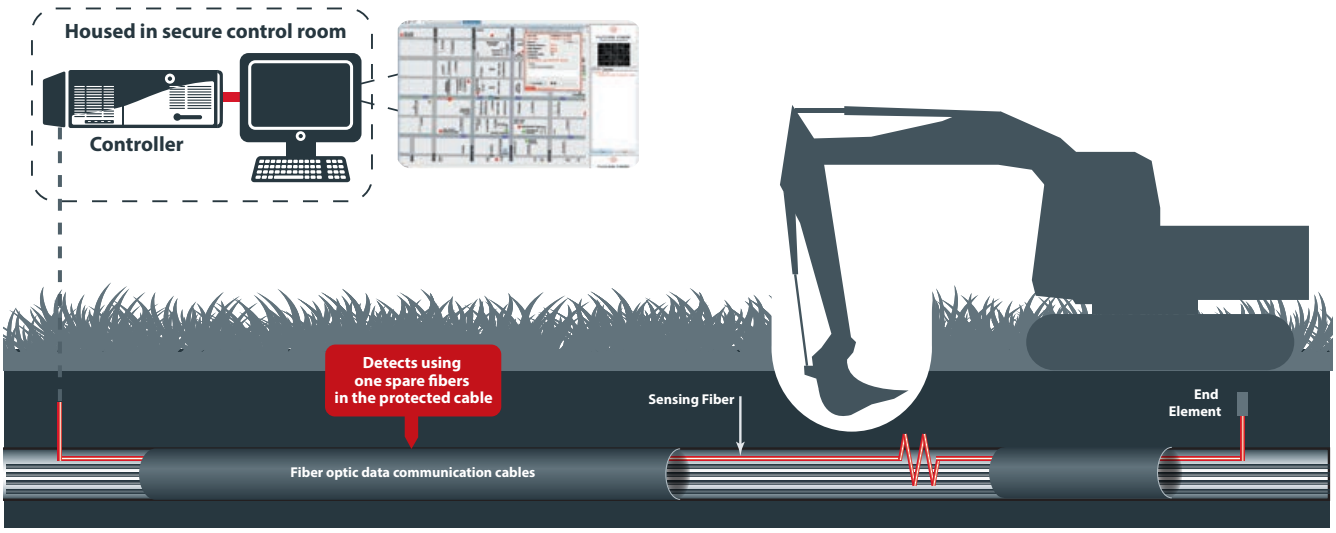
Aura is a high-performance distributed fiber optic sensing system that delivers exceptional performance and operational flexibility. Aura Long Range (LR) monitors longer distances of up to 40km; which is ideal for telecom projects, point-to-point links, and metro area networks. Aura Short Range (SR) supports distances up to 18km (11 miles) and is suited to similar projects of smaller scope.

Aura detects, classifies, and accurately reports the location of a network intrusion with an exceptionally high degree of accuracy. Aura detects to within 6 meters along the sensing path. Aura can also detect activity in the vicinity of the sensor. For example, vehicles, mechanical excavation, manual digging, and even walking can be detected, depending on the application. For critical communications links, the ability to detect nearby excavation can prevent a devastating cable cut due to unintentional construction work near a critical communications segment.

In the event that the sensor cable is severed, the Aura system alerts on the location of the cut and continues to operate up to the cut. An optional configuration supports dual controllers so that the system continues to operate even after a single cut of the sensing cable.

FEATURES

- Single controller supports sensing for up to 40km
- Multiple controllers provide virtually limitless monitoring distances
- Flexible software zones can be changed in minutes
- Locates intrusions to within 6m along the sensor
- Detects manual and mechanical excavation up to 20m from the sensor (depending on soil composition and cable construction)
- Cut resiliency option

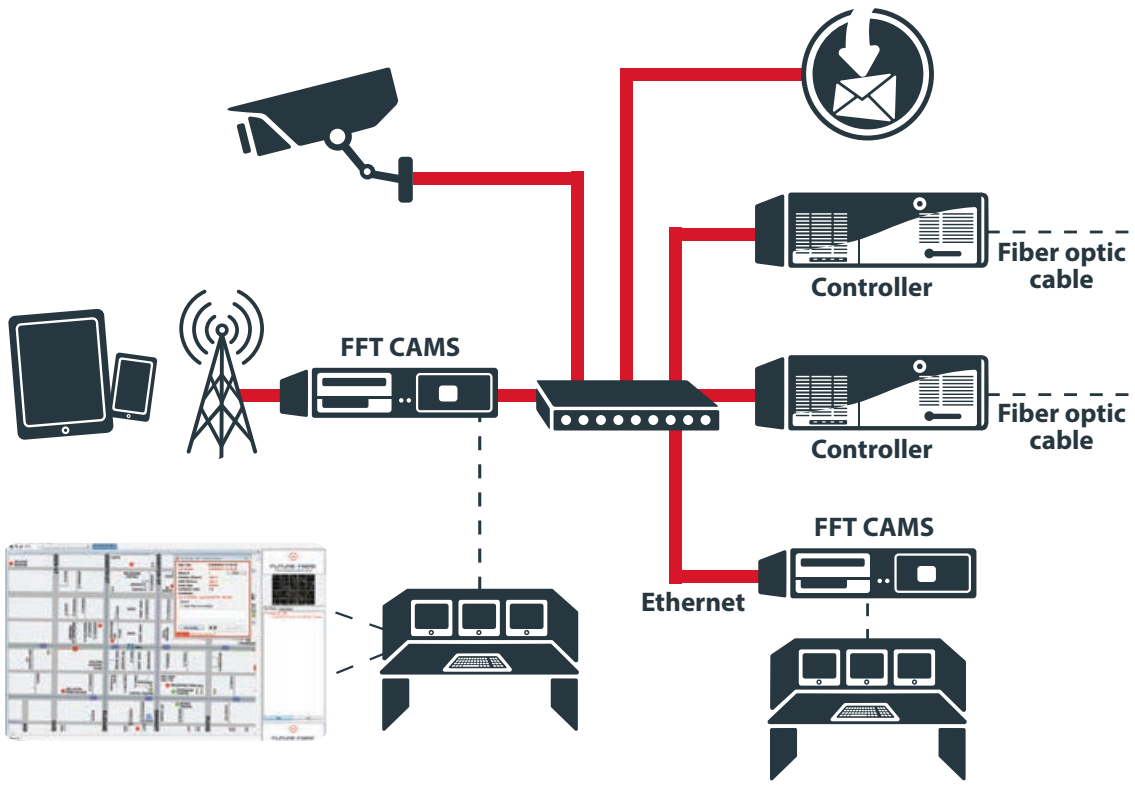


CAMS

CAMS receives inputs from FFT Controllers via ethernet (TCP/IP), and displays alarm and location data. Alarms can be propagated to additional clients, emailed, sent via SMS, or forwarded to an external management application via SNMP trap, SDK integration, or contact relay.

FEATURES

- Intuitive Windows-based Management Application
- Exports SNMP traps to external systems
- SDK integration to external systems available
- Accepts external inputs for inclusion on alarm map
- Supports all FFT controllers – Secure Link, Secure Point, FFT Aura
- Single user interface supports hundreds of miles of distributed FFT sensors
- Available in English, Arabic, French, Russian, Spanish, Japanese, and Chinese



AT A GLANCE

KEY FEATURES ACROSS ALL FFT SOLUTIONS

- Simple and consistent architecture
- Reliable and fast intrusion detection
- No electronics or power required for sensor
- Immune to EMI, RFI, and lightning
- Common alarm interface across all solutions
- Virtually maintenance free

ABOUT FFT

- 20+ years of R&D focused on security applications
- Global leader of fiber optic sensing and security
- Key applications include networks, facility perimeters, oil and gas pipelines
- Sales and support offices around the globe:
  - Melbourne
  - San Francisco
  - Washington
  - Miami
  - London
  - Johannesburg
  - Dubai
  - New Delhi
  - Singapore
  - Istanbul

FUTURE FIBRE
TECHNOLOGIES

www.fftsecurity.com