

Distributed Acoustic Sensing (DAS) vs Conventional Perimeter Intrusion Detection Systems (PIDS)

1. Introduction

The protection of critical infrastructure, industrial facilities, utility corridors, and national borders often depends on **Perimeter Intrusion Detection Systems (PIDS)** to detect unauthorised access or malicious activity.

Traditional PIDS technologies—such as IR beams, buried sensors, microwave barriers, radar, and point detectors—have long been used as part of layered security architectures. More recently, **Distributed Acoustic Sensing (DAS)** has emerged as a powerful distributed alternative or complement for wide-area intrusion detection.

While both approaches address perimeter security, they differ significantly in architecture, coverage, detection philosophy, and operational capability. This guide compares optical fiber DAS against conventional PIDS and helps identify where each technology fits.

2. What is Conventional PIDS?

Perimeter Intrusion Detection Systems (PIDS) typically use dedicated sensors deployed at specific locations or zones to detect intrusion attempts.

Examples include:

Fence-Based Systems

- Copper based fence disturbance sensors
- Coaxial cable based microphonic vibration sensors

Detect:

- Climbing
- Cutting
- Lifting
- Fence tampering

Buried Detection Systems

- Buried cable sensors
- Seismic sensors
- Pressure-based systems

Detect:

- Walking

- Vehicles
- Digging
- Buried intrusion activity

Volumetric Detection Systems

- Microwave barriers
- Infrared barriers
- External PIR's
- LiDAR
- Radar systems

Detect:

- Movement through protected zones
- Approaching intruders
- Vehicle or human activity

3. What is DAS?

Distributed Acoustic Sensing (DAS) uses optical fiber as a continuous distributed acoustic and vibration sensor.

Rather than deploying many individual sensors, the fiber itself becomes a continuous detection element.

DAS can monitor:

- Fence lines for climbing, cutting, lifting and tunnelling
- Buried approach zones for walking, vehicles, digging, etc
- Extended borders for illegal crossings
- Pipeline corridors for encroachment into secure right of way
- Large site perimeters
- Existing fiber routes (where suitable)

It effectively creates a continuous linear sensor over long distances.

4. Key Difference in Detection Philosophy

Conventional PIDS

Typically based on:

- Multiple individual sensors
- Point or segment detection
- Layered sensor deployment

Security coverage is built from many devices.

DAS

Typically based on:

- Continuous distributed sensing with no blind spots
- Single fiber acting as thousands of sensing points
- Event detection across the full route
- High location accuracy to facilitate fast response

Coverage is inherently continuous.

5. DAS vs Conventional PIDS Comparison

Feature	Conventional PIDS	DAS
Detection coverage	Point / zoned	Continuous distributed
Long-range perimeter monitoring	Moderate	Excellent
Event localisation	Moderate	High
Excavation / digging detection	Some technologies	Strong
Wide-area corridor monitoring	Limited to architecture	Strong
Field electronics required	Extensive	None
Field civil works	Extensive	None
Existing fiber leverage	No	Often yes
Event classification analytics	Varies	Advanced
Scalability for long distances	Moderate	Excellent

6. Where Conventional PIDS Performs Well

Conventional PIDS can be highly effective for:

- Compact facility perimeters
- Layered point-security architectures
- Applications needing established legacy technologies
- Sites where security is not considered an operational risk

Often well suited where:

- Perimeters are relatively contained, straight with open sight lines
- Traditional layered systems already exist
- Security architecture emphasises multiple overlapping technologies

7. Where DAS Adds Strong Value

DAS often provides strong advantages for:

Long Perimeters

Examples:

- Airports and Seaports
- Utility sites
- Military sites
- Large industrial campuses

Border Security

DAS is particularly strong where boundaries extend over long distances.

Remote Infrastructure Corridors

Examples:

- Pipelines
- Utility corridors
- Remote assets

Excavation and Underground Threat Detection

A major differentiator in many applications where digging and tunnelling detection is required.

8. Key DAS Advantages Over Conventional PIDS

Continuous Coverage

No gaps between discrete sensors.

Long-Distance Scalability

Can monitor tens of kilometres from one interrogator.

Reduced Field Infrastructure

Often minimal powered field devices.

Intelligent Event Classification

Advanced analytics can help distinguish between:

- Human activity
- Vehicles
- Digging
- Environmental noise
- Threat events

Supports reduced nuisance alarms.

Multi-Function Potential

Same fiber may support:

- Perimeter intrusion detection
- Corridor security
- Excavation detection
- Infrastructure disturbance monitoring

9. Where Conventional PIDS May Still Be Preferred

Conventional PIDS may be preferred where:

- Very short perimeter sections are being protected
- Existing systems already meet requirements
- Simpler detection objectives are sufficient

Technology choice remains application dependent.

10. DAS as a Complement to Traditional PIDS (Not Just an Alternative)

In many projects, DAS is not a replacement but an enhancement.

Examples:

Layered Security Example

- Fence PIDS for initial perimeter breach detection
- DAS for buried approach zone monitoring – pre alarm
- Cameras for visual verification
- Radar for wider situational awareness

This layered model is increasingly common for high security sites.

11. Common Evaluation Criteria

When comparing DAS and conventional PIDS, users often assess:

Detection Performance

- Probability of detection
- Nuisance alarm rate
- Event classification capability

Coverage

- Length of perimeter
- Terrain complexity
- Blind spot risk

Operational Considerations

- Installation complexity
- Maintenance burden
- Field electronics exposure
- Scalability

Integration

- Video management systems
- Command-and-control systems
- Security information platforms
- Existing PIDS infrastructure

12. Typical Application Fit

Application	Typical Fit
Small secure facility	Conventional PIDS
Large industrial perimeter	DAS or hybrid
Border monitoring	DAS
Pipeline corridor security	DAS
High-security layered perimeter	Hybrid
Fence-only intrusion detection	Conventional PIDS or DAS

Increasingly, hybrid approaches are common.

13. Common Misconceptions

“DAS replaces all PIDS”

Not necessarily – depends on budget and site size.
Often it complements existing systems.

“PIDS always has lower false alarms”

Depends heavily on technology and analytics.
Modern Ai driven DAS classification can outperform traditional PIDS very effectively. And has a high probability of detection.

“DAS is only for pipelines”

Incorrect.
DAS is increasingly used across broader security applications.

14. When DAS Is Often the Better Fit

DAS is frequently compelling when you need:

- Very long perimeter coverage

- Remote or harsh environments
- Digging threat detection
- Low field infrastructure
- Existing fiber utilisation
- Distributed security plus analytics
- Scalable corridor protection

15. Conclusion

Conventional PIDS and DAS both play important roles in perimeter security.

Conventional PIDS remains effective for many traditional smaller perimeter applications.

Distributed Acoustic Sensing extends security monitoring into continuous, intelligent, long-range distributed detection.

Rather than viewing them as competing technologies, many modern security architectures use DAS alongside conventional PIDS as part of a layered security strategy.

The right solution depends on threat model, site characteristics, and operational objectives.

16. Further Information

For guidance comparing DAS with conventional perimeter intrusion detection technologies, or selecting the right architecture for your security application, contact fotas@samm.com