

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Serial Connection



# DPAM

Digital Performance and Alarm Monitoring System  
for 2.048 Mbit/s digital networks

As a national or private telecommunications service provider, your wealth is directly proportional to the effectiveness of your network. Network malfunctions are not only expensive in terms of repairs, but with increasing deregulation in the case of national operators, their heaviest costs could be reflected in the number of lost customers.

DPAM is a highly cost-effective Digital Performance and Alarm Monitoring system designed to help you maximise revenue from your telecommunications network through sustained traffic density. Real-time performance trends will help you rectify malfunctions before they become service-affecting and alarm status reporting will allow you to respond to emergencies as they occur.



TCP-IP/UDP

IP Connection

The business of service in telecommunications is becoming increasingly competitive and complex. To be profitable, operators need to have a finger on the pulse of their networks in order to maximise their efficiency through the early detection of malfunctions or performance degradations.

## Your business benefits

Your network isn't buried somewhere in a machine shop where it's failure would go unnoticed by your customers. It's right out there for the world to see - and to use. Your network is your business and the health of both is directly related to satisfying client needs. By exhaustively monitoring your 2Mbit/s links, DPAM will contribute to your business health in the following ways:

### Improved revenue

- **Maximised income from sustained traffic density:** Inoperative links are simply an expensive overhead.
- **Satisfied and therefore retained customer base through service level agreements and reduced network downtime:** This is specially relevant in the case of hard-earned, high-volume clients such as banks and corporates who insist on guaranteed up-time and rapid rectification of errors.
- **Better competitive position:** Improved confidence in selling of services

### Reduced maintenance costs

Rigorous monitoring and the early detection of trends contribute to significantly reduced operating costs:

- **Standard operating procedure:** The more routine the maintenance, the more cost-effective it becomes.
- **Proactive rather than reactive maintenance:** Early detection of malfunctions contributes to controlled rather than emergency situations and provides for the addressing of problems before they become service-affecting.
- **Pinpointing of exact failure location:** The rapid and exact location of network failures drastically reduces trouble-shooting times and costs.

### Improved asset management

- **Cost-effective care of costly transmission assets:** DPAM represents a high return to expenditure ratio when considering the cost of the equipment in its care.
- **Improving the odds:** By helping to pinpoint the source of problems, DPAM helps to reduce the number of weak links in the service delivery chain.

## About DPAM

The DPAM system is a bi-directional, intrusive error analyser for the testing and monitoring of 2.048 Mbit/s digital circuits compliant with ITU-T M.2120 recommendations. All 2 Mbit/s error information is based on either Frame Alignment Signal (FAS) or Cyclic Redundancy Check (CRC).

Together with the 2 Mbit/s error and network performance information (ITU-T G.826), system auxiliary alarms can also be monitored. All errors are presented to the Element Manager as UDP LAN data which, in turn, could be forwarded to a user-provided National Network Operating Centre (NNOC) for alarm and performance data indications.

For ease of reference, the following product codes are used in this document:

|                          |  |
|--------------------------|--|
| <b>PM-IFR</b>            | 19" Intrusive Sub-rack with capacity for 14 monitoring boards and dual 48VDC input supplies (redundancy) |
| <b>PM-IPU</b>            | Sub-rack Power Supply Unit   |
| <b>PM-CFL</b>            | Sub-rack Controller Card with Equipment Craft Terminal port and LAN Network Management port              |
| <b>PM-IFM</b>            | Intrusive Master Card  |
| <b>PM-IXM</b>            | Auxiliary Alarm Master Card  |
| <b>PM-IFBP</b>           | Remote Motherboard Enclosure indoor  |
| <b>PM-IFS</b>            | Intrusive Slave Card indoor  |
| <b>PM-IFXS</b>           | Auxiliary Alarm Slave Card indoor  |
| <b>PM-IFMC</b>           | Intrusive Micro-cell Enclosure (includes battery and charger) outdoor                                    |
| <b>PM-IFS-MC</b>         | Intrusive Slave Micro-cell Card outdoor  |
| <b>PM-IFXS-MC</b>        | Auxiliary Alarm Slave Micro-cell Card outdoor  |
| <b>INA-DPAM-1400-001</b> | Windows® NT or 2000 Global Element Manager   |

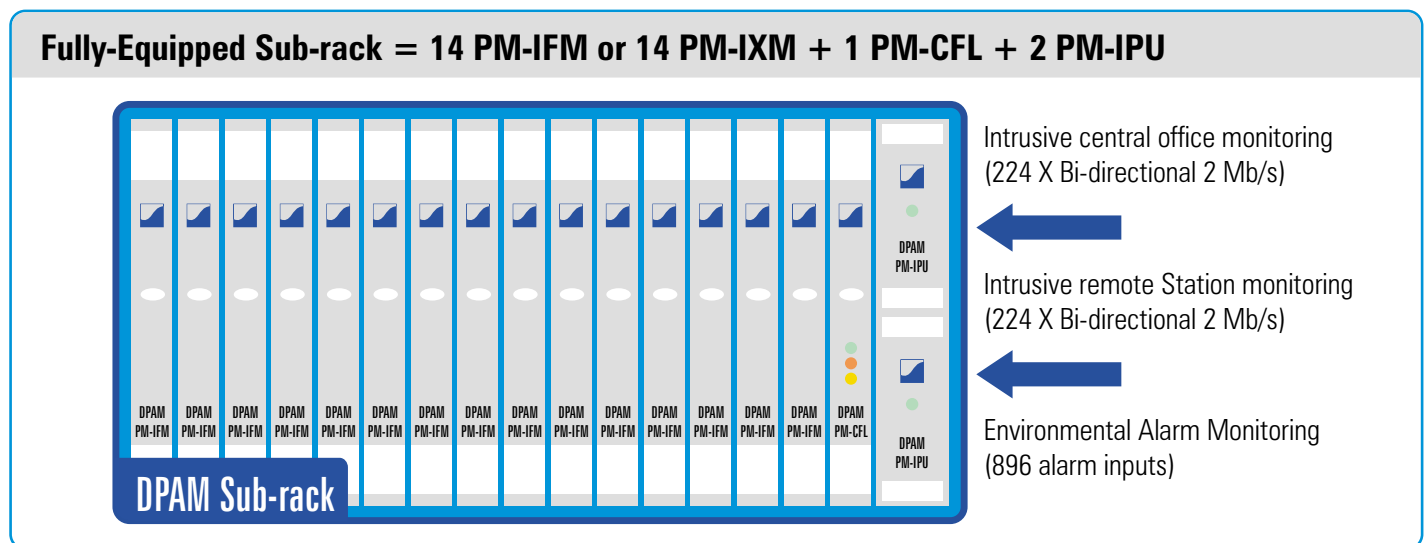


Figure 1

## The DPAM system comprises the following:

### Central Office Unit (PM-IFM or PM-IXM):

As shown in the above diagram, the central office sub-rack has the capacity for up to 14 Intrusive Master monitoring (PM-IFM) cards or up to 14 Auxiliary Alarm Cluster (PM-IXM) cards and one Communications Controller (PM-CFL) card. The sub-rack also houses two redundant Power Supply (PM-IPU) cards.

Each PM-IFM card can monitor up to 32 bi-directional E1 circuits either locally or remotely, using the monitored E1 circuit, spare SA bits, for communication between the local and remote sites.

Each PM-IXM card can monitor up to 64 environmental alarm inputs, either static (on/off), pulsed or optionally analogue level measurements.

### Remote station indoor monitoring (PM-IFS):

For indoor applications, the Remote Motherboard Enclosure unit consists of a plastic enclosure (PM-IFBP) with a capacity for up to 5 Intrusive Slave Monitoring (PM-IFS) cards or up to two Auxiliary Alarm Slave (PM-IFXS) cards each connected to a PM-IFS card for alarm monitoring expansion purposes.

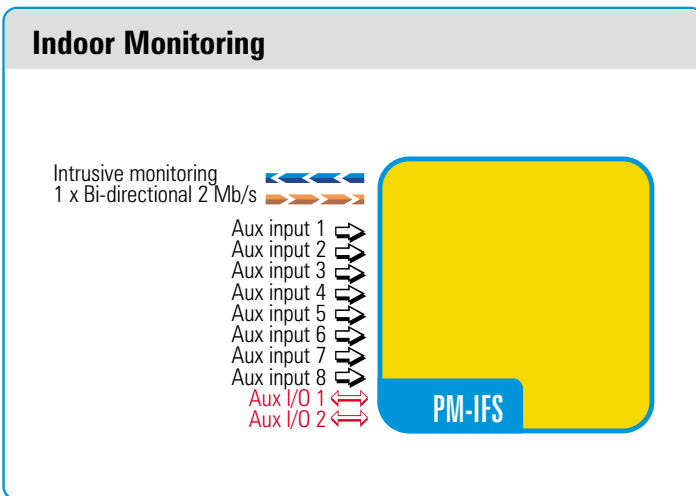


Figure 2

Each PM-IFS is connected to a master PM-IFM monitoring card via the monitored E1 circuit. The PM-IFS can monitor one bi-directional E1 circuit as well as ten environmental alarm inputs. Two of these inputs can be configured for outputs such that they can be used for control purposes.

### Remote station expanded alarm monitoring (PM-IFXS):

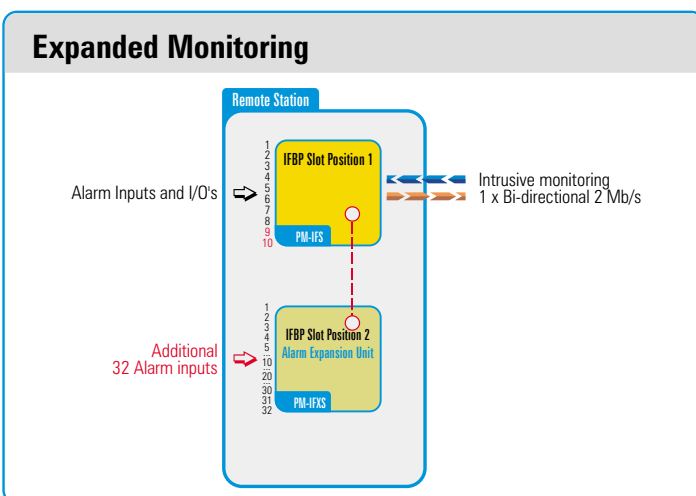


Figure 3

Should the 10 alarm inputs associated with the PM-IFS be insufficient, the PM-IFXS can be connected as an expansion module to provide an additional 32 inputs for a total of 42 alarms, either static (on/off), pulsed or optionally analogue level measurements.



Remote Motherboard Enclosure

### Remote station outdoor monitoring (PM-IFS-MC):

For outdoor applications, the remote Micro-cell unit consists of a metal enclosure (PM-IFMC) with a capacity for 2 Intrusive Slave Micro-cell (PM-IFS-MC) cards or one Auxiliary Alarm Micro-cell (PM-IFXS-MC) card connected to a PM-IFS-MC card (alarm monitoring expansion purposes).



Remote Micro-cell Enclosure

## Some possible DPAM applications

### Corporate application Point to Point

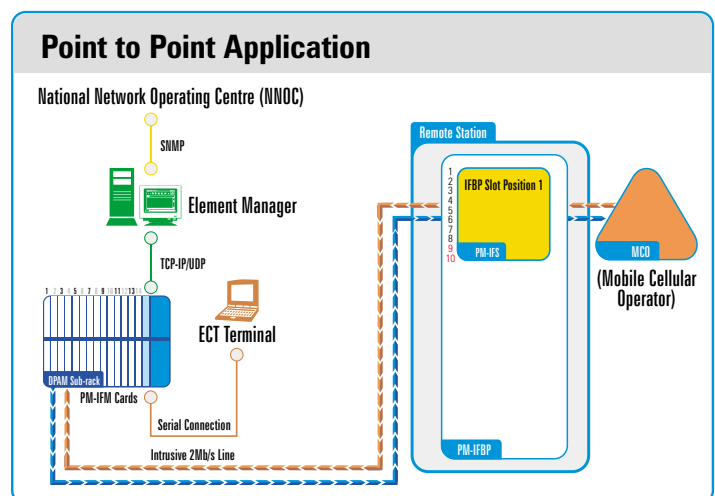
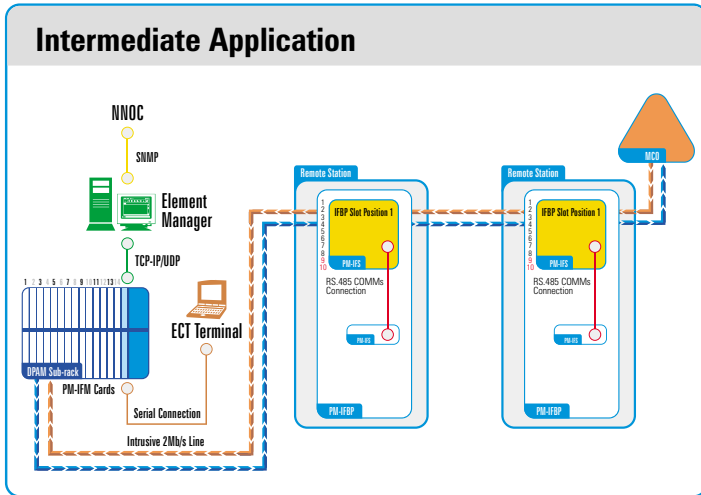


Figure 4

In the point to point scenario, each PM-IFM card is capable of monitoring the local end of 16 bi-directional 2Mbit/s circuits as well as the remote end of 16 bi-directional 2Mbit/s circuits (32x 2Mbit/s circuits) via the intrusive slave boards (PM-IFS).

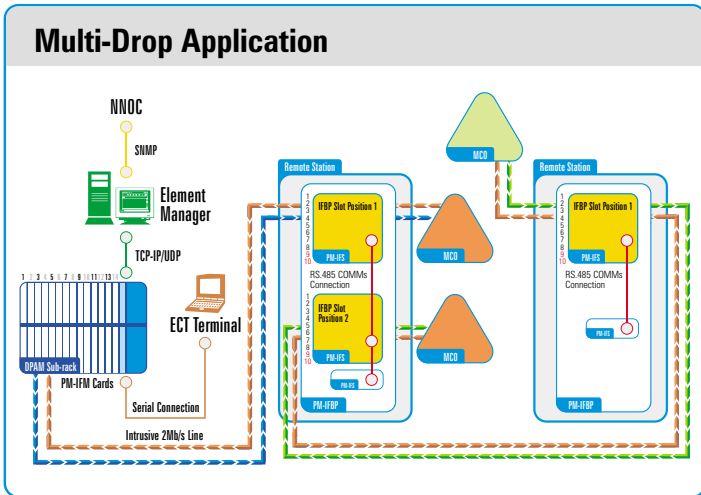
**Microwave application Intermediate alarm monitoring**



**Figure 5**

In a multi-drop scenario each remote PM-IFS represents the monitoring of a different 2Mbit/s circuit. The PM-IFM is also capable of monitoring remote 2Mbit/s circuits of the same origin. It means that various PM-IFS units could be multi-dropped but utilising the same 2Mbit/s circuit through each remote location.

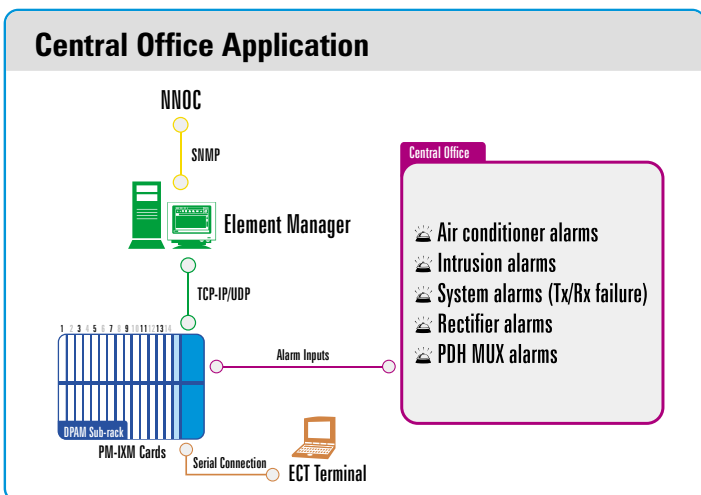
**GSM application Multi-drop or Star**



**Figure 6**

The PM-IFM also has the capability of monitoring remote station 2Mbit/s circuits only, in a multi-drop scenario. In this application it is possible for the PM-IFM to communicate intrusively via the imbedded SA bits to the remote station PM-IFS units in a multi-drop scenario with up to 31 remote PM-IFS units. (the 1<sup>st</sup> circuit being used for termination at the local CO site total 32 circuits)

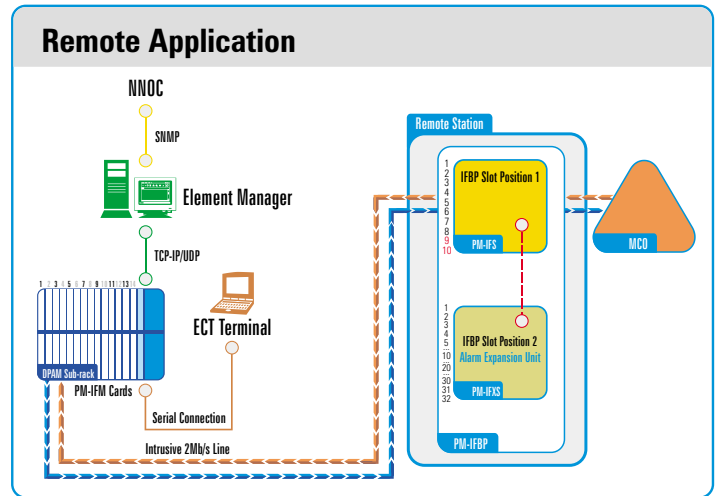
**Environmental alarm monitoring application central office**



**Figure 7**

The PM-IXM card is a Central Office 19" sub-rack mounted module. Each PM-IXM environmental alarm-monitoring card has 64 individual ports for auxiliary alarm collection. Each port can be configured for static (on/off), high speed pulsed monitoring or optionally analogue level measurements. Static alarm inputs such as air conditioner, intrusion, rectifier and system alarms Pulsed alarm inputs such as PDH MUX alarms 8Mbit/s, 34Mbit/s and 140Mbit/s Analogue alarm inputs such as battery voltage and temperature

**Environmental alarm monitoring application remote station**



**Figure 8**

Each PM-IFXS can only operate through a PM-IFS unit, thus expanding the possible auxiliary alarms to be monitored with up to an additional 32 alarm inputs. The interconnection between the PM-IFS and the PM-IFXS is done via an on-board fly-lead (RS.485), which provides power and communications to the PM-IFXS. Each PM-IFXS is capable of monitoring 32 digital alarm inputs, either static (on/off), high speed pulsed monitoring or optionally analogue level measurements. Static alarm inputs such as air conditioner, intrusion, rectifier and system alarms Pulsed alarm inputs such as PDH MUX alarms 8Mbit/s, 34Mbit/s and 140Mbit/s Analogue alarm inputs such as battery voltage and temperature (1x PM-IFS = 10 Auxiliary alarms + 1x PM-IFXS = 32 Auxiliary alarms, thus a total of x42 Auxiliary alarm inputs for a PM-IFS/IFXS combination)

All digital alarm information from the PM-IFXS is transferred together with all the 2Mbit/s performance (G.826) and alarm information (M.2120) of the PM-IFS to the PM-IFM via the intrusive 2Mbit/s circuit.

**Business benefits:**

- Save time by rapidly pinpointing the exact fault location (this is specially valuable in rural areas)
- Retain satisfied customer base
- Optimise the usage of expensive Cellular Operator assets by predicting malfunctions from performance trend analyses
- Reduce the number of costly emergency repairs
- Unprecedented low-cost, high-density monitoring capabilities
- Win business through guaranteed up-time or short-time-to-repair
- Retain corporate customer business
- Add value by monitoring alarms such as intrusion, security, fire, equipment malfunction, asset tampering, etc.
- Convenient access to other links contributes to fast and low-cost installations

# Global Element Manager (GEM)

The Global Element Manager seamlessly integrates any remote device with existing National Network Operator (NNOC) initiatives. Whether you're operating in the Windows 98® 2000® or NT® environments, GEM was designed for ease-of-use and provides flexible fault, configuration and performance management of the monitored 2 Mbit/s circuits.

## About GEM

- GEM is an alarm monitoring system designed to address the issue of facilities management of remote sites, typically cellular BTS sites of virtually any size or complexity.
- GEM can manage a wide variety of 2 Mbit/s circuits and alarm inputs.
- GEM caters for both local (Central Office) and remote (BTS sites) monitoring/management.

Unparalleled configuration flexibility combined with low cost and high port density means that GEM could be configured to cope cost-effectively with the smallest to the largest monitoring applications.

## GEM FCAPS MODEL

### Fault Management

**Information and event log** - this includes the complete listing of all alarms, failures, performance thresholds, etc.

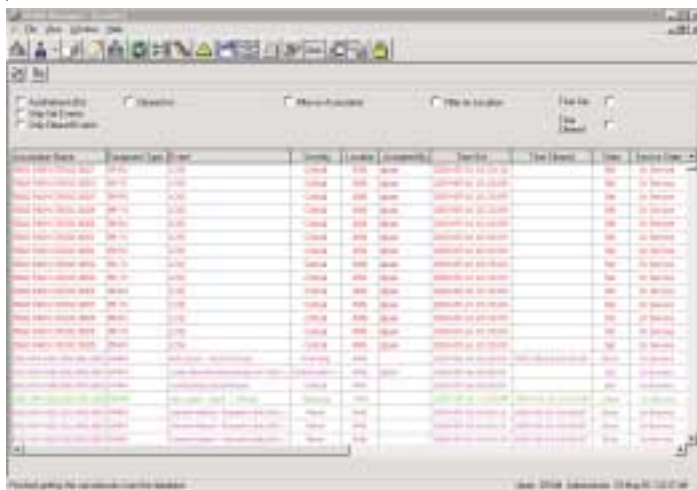
**Log report customisation** - to get to relevant information as quickly as possible, the system caters for the screening and filtering of event and history logged data.

**Alarm classification** - alarms are categorised as *critical*, *major*, *minor*, *warning*, *indeterminate* and *cleared*.

**Alarm indication setting** - provision is made for the selection of audible or visual alarm indications.

**Failure notification** - this includes details such as time, date, severity, specific problems, trouble description, etc.

**Event / Alarm surveillance** - this provides real-time supervision of network elements and the monitored sections of the network as well as alarm and performance failures.



### Configuration Management

**Equipment provisioning** - this is used for the commissioning of equipment or to re-install equipment after repair. It's also used for stand-by or reserved equipment.

**NE configuration** - this provides for the full configuration of all the network elements in the network.

**NE administration** - this includes setting of the systems clock, backing-up files, archiving and downloading software.

**NE database management** - functions include initialising, re-initialising, updating, backing-up and querying.

**NE status and control** - this can be scheduled beforehand or done on demand.

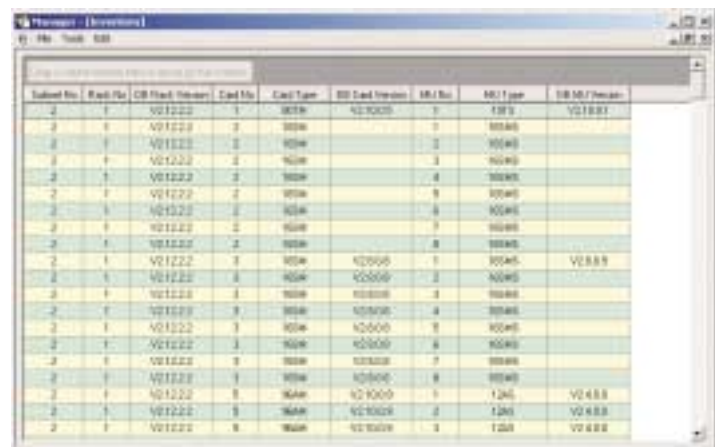
**System configuration database** - the code, type and serial number as well as the hardware and software revision dates of the equipment in use is stored in this database.



### Accounting Version Control

**Accounting database Total Inventory** can be viewed, which refers to all version numbers ranging from the GNE to the NE. Subsequently card inventory can be viewed, which refers to all GNE related version numbers.

This feature is very useful to ensure that all hardware responsible for monitoring conforms to the latest release of firmware and hardware version control.



### Performance Management

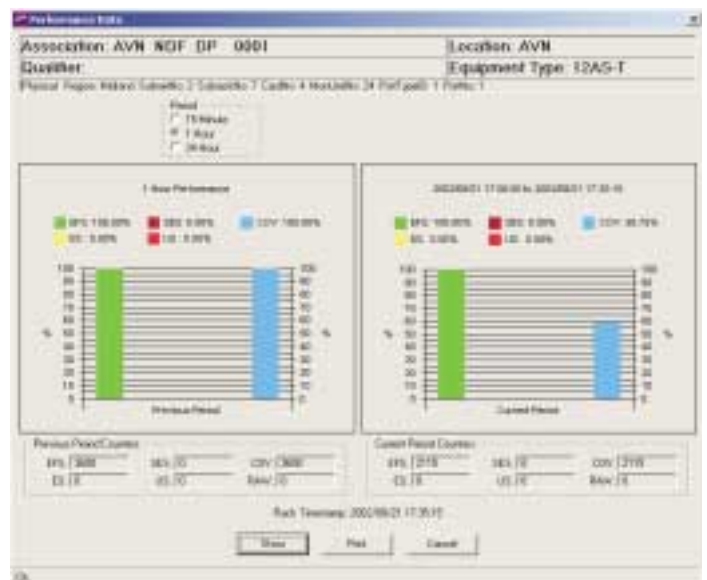
**Information at a glance** - the system provides for graphical views of performance and statistical data for easy and quick analysis.

**Performance monitoring** - this can be done on demand or scheduled for 15 minute, hourly or daily intervals.

**Historical performance log** - the frequency of logging can be set for 15 minute, hourly or daily intervals.

**Threshold setting** - the performance of network elements is compared to set threshold limits for the type of equipment being used.

**Missing information handling** - unavailable time is logged and time stamped.



## Security Management

GEM User Profiles these are created as users part of pre-defined user groups. Each GEM user is created by the system administrator with various rights, which is determined by the user group.

Each user has a unique user name and password. Each user group is allocated various rights regarding monitoring and configuration through a selectable template.



## Conformance with international telecommunications standards

DPAM conforms to the following international telecommunications standards:

1. ITU-T Rec G.703  
E1 Signal Physical Characteristics
2. ITU-T Rec G.704  
E1 Frame Structures
3. ITU-T Rec G.823  
The control of jitter and wander within digital networks which are based on the 2048Kb/s hierarchy
4. ITU-T Rec G.821  
Error Performance of an international digital connection operating at a bit rate below the primary rate and forming part of an integrated services digital network
5. ITU-T Rec G.826  
Error Performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate
6. ITU-T Rec G.706  
Frame Alignment and Cyclic Redundancy Check (CRC) procedures
7. ITU-T Rec M.2120  
PDH/SDH Path Fault Detection and Localisation Procedure (Alarm Filtering)
8. ETS 300 019-1-3 February 1992  
Equipment Engineering, Environmental conditions and environmental tests for telecommunications equipment Part 1-3: Classification of environmental conditions Stationary use at weather protected locations
9. IEC 68-2-1 Fifth edition 1990-04  
Basic environmental testing procedures. Part 2 Tests - Test A. Cold

10. IEC 68-2-14 : 1984

Basic environmental testing procedures. Part 2.1 Tests - Test N. Change of temperature.

11. IEC 68-2-2 : 1974

Basic environmental testing procedures. Part 2.1 Tests - Test B. Dry Heat

## The next step

By putting you firmly in control of your transmission network and its valuable assets, DPAM will directly contribute to your bottom line and can make the difference between vital profitability and mediocrity. Contact us today to see how DPAM will help your business cope with the network technological and competitive challenges of the 21st century.

## Inala Systems Division

**A division of Inala Technologies (Pty) Ltd.**  
Reg. No. 2004/007308/07

**Call Centre**  
Toll Free: 0800 117850  
Fax: +27 11 206 8451  
callcentre@inala.co.za

## Gauteng

**Sales**  
557, 15th Road,  
Randjespark,  
Midrand,  
South Africa.

Private Bag X131,  
Halfway House,  
Midrand,  
1685,  
South Africa.

Tel: +27 11 206 8360  
Fax: +27 11 206 8451  
info@inala.co.za

<http://www.inala.co.za>

