

Overview of



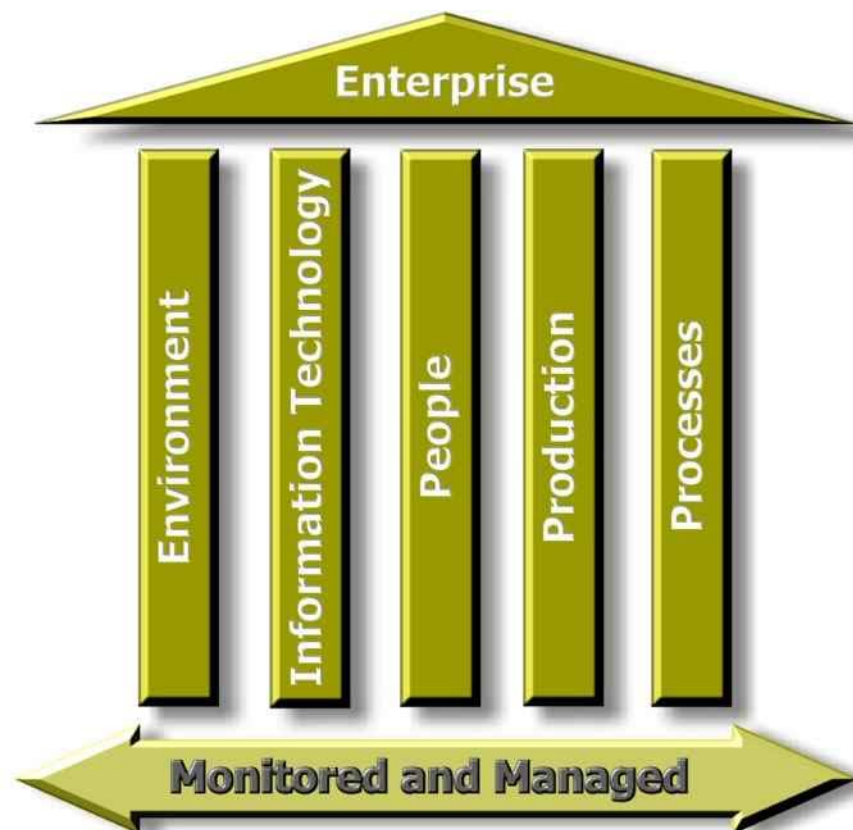
RARS and Enterprise Monitoring

Traditionally Enterprise Monitoring referred to the monitoring of the IT Infrastructure in an organisation.

In today's competitive environment a more integrated and holistic approach is needed to leverage the corporation's investment in computing services, people, systems and processes.

Enterprises exist to provide products and services in the most competitive way. To remain competitive companies have to ensure the seamless and smooth delivery of each process that is in effect to make up the finished product or the level of service that is rendered.

It is therefore important to not only address the traditional IT functions, but to also look more closely at the pillars that make up the business environment.



The Environment

The monitoring and reporting requirements within different business environments vary as much as the businesses do. As an example, what need to be monitored and recorded will differ substantially between a manned data centre, a disaster recovery site and a remote, unmanned BTS site.

With RARS we have developed the software and hardware elements that address the vast array of environmental monitoring requirements that different locations, applications and unique surroundings are necessitating.

Environment monitoring in computer rooms, data centres and BTS sites has become a critical part of disaster prevention. The reason is that a typical IT infrastructure supports the entire organisation. Without continued operation of IT resources, an organisation may have no access to information, databases, email or the internet. Even worse, an organisation may appear to be *'out of business, unstable'* or simply *'irrelevant'*. During downtime, costs continue to accrue while more and more profits are lost.


The biggest threat continues to be air conditioning failure or improper cooling that causes temperature and humidity extremes. Second to this are the risks of fire and the interruption of the power supply that causes system failure if not handled properly. Then there is the risk of intrusion, theft and tampering by unauthorised personnel.

With these primary concerns threatening every organisation, there are easy, inexpensive and proven solutions available to prevent environment caused disasters.

The computer room, data centre or BTS site *'environment'* means the physical conditions that may cause problems if they exceed certain thresholds. The primary environment conditions that typically need to be monitored include:

- **Temperature** (e.g. air conditioning or ventilation problems)
- **Humidity** (e.g. air conditioning, water or ventilation problems)
- **Power** (e.g. Main or UPS power loss, start, consumption)
- **Generators** (e.g. Diesel/fuel level monitoring, start/stop times monitoring, run-time estimating)
- **Flood/Water** (e.g. air conditioning, plumbing or roof leak)
- **Smoke/Fire** (e.g. electronics burning or room fire)
- **Air Flow** (e.g. are air conditioners or cabinet fans moving air)
- **Room Entry** (e.g. unauthorized room or cabinet entry)
- **Panic Button** (e.g. user or security presses panic button)

The EnviroRAMM units were specifically designed and manufactured to address the unique requirements of each installation, and a suite of RAMM products are available for environment monitoring of computer rooms, data centres, plants or other facilities. It detects problems with air conditioning, power supply and other critical issues that are major threats to large systems or data centre environments. Environment sensors built into or attached to the RARS RAMM units will dynamically monitor temperature, humidity, main and UPS power, flooding, smoke/fire, intrude/entry, panic buttons and more.

	SMS	TCP/IP	Analogue	Digital - In	Digital - Out	Display	Camera	Battery	Configuration	Control	Audits	Reports	SLAs
RAMMSMS ⁸	✓	✗	✗	8	8	✗	✗	✓	✗	✗	✗	✗	✗
RAMMSMS ¹⁶	✓	✗	4	16	16	✗	✗	✓	✗	✗	✗	✗	✗
RAMMNet	✗	✓	✗	16	16	✗	✗	✗	✗	✗	✗	✗	✗
hyperRAMM	✓	✓	4	12	10	✓	✓	✓	✓	✓	✓	✓	✓
EnviroRAMM [®]	✓	✓	4	12	10	✓	✓	✓	✓	✓	✓	✓	✓

Full alert notification is available on all units, and automatic corrective action are available to shut down servers, move files, re-route processing, start fans or backup air conditioners, and initiate other appropriate automatic responses on specific units.

The reason environment monitoring in the computer room is critically important is because computer and network equipment is only designed to operate within a specific range of environmental conditions. If these conditions exceed reasonable limits, unpredictable and potentially catastrophic results will occur, such as damaged equipment, disk failures, CPU errors, system crashes, data loss, fire or worse. Most equipment manufacturers, as well as maintenance and support vendors, will not accept responsibility for problems caused by equipment which has been damaged by extreme temperature, humidity, flood, loss of power, etc.

Preventing just one environmental event typically cost justifies the deployment of RARS the first time a catastrophe is avoided. Think about the cost of your data centre, computer room or BTS site being down for an hour, let alone a day or even a week.

How much would it cost your organisation?

Can you prevent it?

Who gets the blame if you cannot?

[Information Technology – RARS Platform Monitoring Agent](#)

In today's business environment, a company's data is its lifeblood. Once the exclusive realm of large corporations, servers and applications with mission-critical data have become commonplace in small and medium businesses. Avoiding downtime is especially critical for smaller businesses and IT sites, because they are less likely to have the staff, resources or disaster-planning capabilities of larger computer installations.

The RARS Monitoring Agent is a service which is installed on WIN32 (Window NT/4, Windows 2000/3 and Windows/XP) platforms.

The RARS Platform Monitoring Agent performs the following functions:

Reporting Targets

Any information and alarm information may be sent to RARS Servers and other hosts via SMTP Email and SNMP traps. Any number of reporting target hosts may be defined. Heartbeats are Reporting Target hosts in a predefined interval.

Windows log filters

Each windows platform has multiple logs. (I.e. Application, Error and Security log) other logs are available depending on configuration. Messages written to these logs may be monitored and filtered. Any message trapped by a matching filter is reported.

File-System Monitoring

The RARS Platform Monitoring Agent monitors user-specified file systems for utilisation and growth between polls. The status of the file system itself is the worst condition reported by the various measures of file-system usage and growth. When the status of the file system itself changes, the RARS Platform Monitoring Agent sends an SNMP trap, reflecting the overall status of the file system.

Each file system is monitored for the amount of file-system space used, which is compared to user-defined warning and critical thresholds. If the detected amount of used space on the file system falls above the warning or critical threshold, the status for the file-system utilisation is set accordingly.

In addition, a file system can also be monitored for the amount of growth in used space between polling periods. If this figure exceeds a user-defined threshold, the status of the file-system growth is set to a user-defined level.

File Monitoring

For a more precise monitoring of file-system usage, the RARS Platform Monitoring Agent can be configured to monitor a number of aspects of overall file size growth, timestamp change, and file growth between polls. The overall growth of a file's size can be monitored against user-specified warning and critical thresholds. If the overall size of the monitored file exceeds a threshold, the status of the file's size is set accordingly. In addition, each file can be monitored for changes to the file, such as in instances in which you would want to detect tampering with files containing sensitive material. Changes in a file's timestamp can be used to indicate changes made to the file. When a timestamp change occurs, a user-defined warning or critical alert can be raised, and the status of the file timestamp set accordingly. Once a timestamp change has been detected, a user can reset the file timestamp status to OK to resume checking for timestamp changes.

To prevent a file's growing at an unexpectedly rapid rate, such as when a large number of error messages would be reported to a log file, the percentage of growth in file size between polls can be compared to user-defined warning or critical thresholds. If the threshold is exceeded, the appropriate status is recorded for file-size change. Once the threshold has been exceeded, a user can reset the file-size change status to OK to resume checking for file-size changes. The overall status of the file reflects the worst condition reported by the various aspects of file size growth and change. When a status change occurs, the RARS Platform Monitoring Agent sends an SNMP trap.

Process Monitoring

The RARS Platform Monitoring Agent allows the user to monitor what is happening (or not happening) on a system. The RARS Platform Monitoring Agent monitors user-specified processes for whether they exist or do not exist on the system. Some processes, for example, must be running for your system to function properly. You would want to be warned as quickly as possible if one of these processes should stop for any reason.

Although monitoring the existence (or non-existence) of a particular process gives some indication of the status of your system, you may want to monitor the behaviour of processes in greater detail, such as for the number of instances of a process or the number of threads.

If a user-defined process is monitored for the maximum number of instances that a process can have, and if predefined warning or critical thresholds are exceeded, the appropriate status is set for the process. This feature is useful, for example, if two instances of a process are allowed to be running on a machine, but more than two would violate a licensing agreement.

At a finer level of granularity, the RARS Platform Monitoring Agent can monitor a particular process instance for the number of threads created. A process may, for example, be expected to have a number of active threads, and a user would want to know if it had fewer active threads, as an indication that the process may not be running correctly.

The overall status of the process reflects the worst condition reported by the various aspects of process activity that the RARS Platform Monitoring Agent is monitoring. When a process's status changes the RARS Platform Monitoring Agent sends an SNMP trap.

Service Monitoring

On a Windows system, the correct services should be running at the correct times. The RARS Platform Monitoring Agent allows the user to monitor whether a service is active or non-active. When a service's status changes the RARS Platform Monitoring Agent sends an SNMP trap.

Memory Monitoring

The RARS Platform Monitoring Agent checks the availability of sufficient memory to provide an acceptable level of service by monitoring the percentage of memory that has been used (memory load), the percentage of physical memory that is available, and the percentage of swap space that is available.

The RARS Platform Monitoring Agent monitors for the percentage of memory that is currently being used and compares it to user-defined warning and critical memory-load thresholds. The memory load must exceed the thresholds for a user-defined number of successive polling intervals, before the RARS Platform Monitoring Agent changes the memory load's status and sends a corresponding trap.

Likewise, the RARS Platform Monitoring Agent compares the amount of available physical memory against user-defined warning and critical available physical memory thresholds. The available physical memory must remain below the thresholds for a user-defined number of successive polling intervals, before the RARS Platform Monitoring Agent changes the available physical memory's status and sends a corresponding trap.

In addition, the percentage of available swap space is compared against user-defined warning and critical available swap space thresholds. The RARS Platform Monitoring Agent does not change the available swap space status and send a trap, until the available swap space falls and remains below the user-defined warning or critical thresholds for a user-defined number of successive polling intervals.

Processor Monitoring

The RARS Platform Monitoring Agent monitors each of the processors in the system for CPU utilisation and compares their current utilisation against user-specified warning and critical thresholds.

When the processor utilisation exceeds a specified warning or critical threshold for a specified number of consecutive polling intervals, the RARS Platform Monitoring Agent records the appropriate status against the affected processor and sends an SNMP trap. Checking a condition for a specified number of consecutive polling periods ensures that the reported status is representative of a persistent problem, such as a process hogging the processor, rather than a short-term problem, such as an utilisation spike caused by a single event.

Registry Monitoring

The RARS Platform Monitoring Agent can be configured to monitor any number of important Registry value entries (or leaves). The way that the Registry value entry is monitored, or watched, is dependent upon its type and the configuration specified by the user. If the

value entry being monitored is an integer, it can be monitored for either a simple, absolute change or monitored for a change in value against user-definable warning and critical thresholds. If the entry is a string, it can be monitored for a change in its contents.

When a value entry is modified, or when it exceeds a warning or critical threshold, the appropriate status change is recorded against the watched Registry value entry, and an SNMP trap is sent. The status of the Registry value entry can be reset by the user to continue monitoring of the value entry.

Event-Log Monitoring

The RARS Platform Monitoring Agent can be configured to monitor for the existence of user-defined events in the Security, System, and Application event logs. Event-log monitoring can be used for general auditing purposes to monitor the number of entries of a specified type in a specified log. It can also be used to monitor for a specific event. For example, an event-log watcher can be defined to monitor for the occurrence of a logon event and raise an SNMP trap, should one be detected. Alternatively, an event-log watcher can be configured to identify the occurrence of failed logon attempts, which can indicate that someone is attempting to compromise the security of a sensitive system.

When the event log is modified, or exceeds a warning or critical threshold, the RARS Platform Monitoring Agent changes the status of the event-log watcher accordingly and sends an SNMP trap sent. The status of the event-log watcher can be reset by the user to continue event-log monitoring.

Available File Systems

The Agent provides information on the file systems that are available for monitoring.

Available Processes

The Agent provides information on the processes that are available for monitoring

File Tailer

The Agent provides the ability to tail text files. The file tailer can monitor an ASCII Text file and access any new messages which are written to the file. Messages matching defined filters may be reported. A list of files may be monitored and any change to the file is reported

Performance Data

Windows provides an API where performance data is accessed. Up to 9800 difference performance counters are available on a simple Windows server. Any counter may be configured for monitoring with thresholds and any out of line information is reported. Counters may be configured to collect statistics which are maintained in a local server table.

The agent collects all performance data on the local machine makes them available for monitoring. The agent may be configured to monitor the processes running on the server. These may be a Service, Driver or program.

Each monitored process is associated with time period rules and whether the process should run on not. Any differences are reported.

Software monitoring

The agent builds a list of installed software and versions. Should the software level of any installed program change it is reported. Any installation and de-installation is reported.

Period Rules

The Agent monitoring capabilities can be monitored based on time and date settings.

People

Support personnel can be both a boon and a burden to a company, either increasing customer satisfaction and return on investment or making customers and technicians miserable. One of the keys to achieving the former is selecting a system that not only fits the company's present and future event logging and call escalation needs, but one that is designed to also make the technicians' jobs more manageable and less complicated.

Functionally, the system should have - at a minimum - first-level responsibility for problem determination and system restoration, and provide the following features:

- Log system failures and malfunctions
- Provide one centralized contact point
- Collect product evaluations from end users
- Track and manage difficult problems
- Provide a way to escalate very serious problems and those that are slow in being resolved
- Identify recurring problems
- Support and manage configuration changes plus inventory tracking in support of information services.
- Generate and use problem history to improve the availability of various systems and equipment.
- Provide management reports for evaluating performance and service-levels

The RARS approach was devolved using a more proactive than reactive approach. We have enhanced our problem detection and reporting capabilities so that support staff can foresee and rectify a problem before it becomes catastrophic.

We are also continuously upgrading and enhancing the user interfaces and transmission media to make it easier and more efficient to report problems, and easier for support staff to retrieve and respond to them.

Production

A manufacturing company may want to improve straight-through manufacturing yields, thus reducing rework. To achieve this goal, the company will need a system to schedule preventive maintenance so that equipment would stay within specified operational parameters and batches would meet all quality requirements.

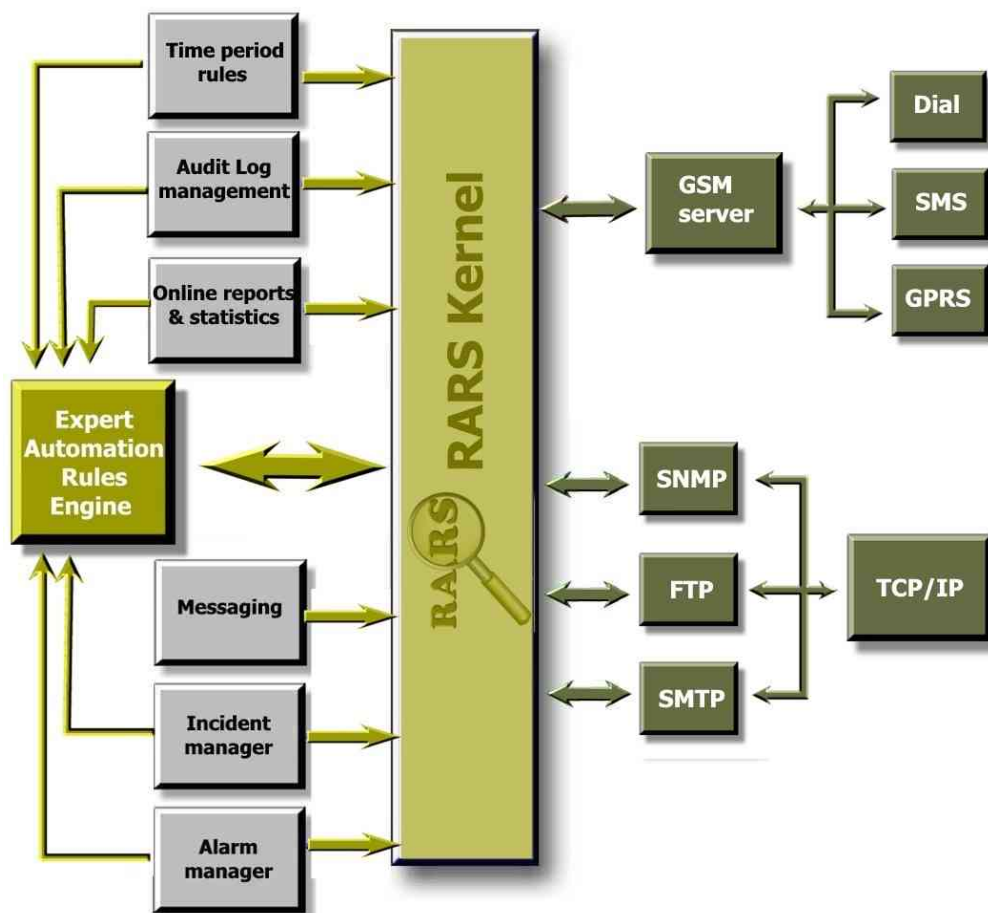
There are many applications on a factory floor that are ideally suited to the RARS monitoring solution set. From the monitoring of the mains power, to managing and interfacing with CNC machines and PLC systems, and the management and scheduling of service level metrics, RARS provides a holistic view of the production environment and the enterprise.

Service-level deliverables refer to the level of service to be provided to the end user in terms of timeliness, accuracy, and reliability. The service level that is provided is often determined by factors identified in the business objectives. Service level deliverables typically are stated in terms of a time frame and the required service as a percentage of total time.

Such objectives, for instance, may state that in order to ensure adequate response, the network response time for this location cannot exceed two (2) seconds, and the network must exceed 99.9 percent availability between 8AM and 8PM.

The RARS Expert facility is an application which provides services for processing input from various sources. Once processed, selection criteria are applied on each input message received. Various actions based on information presented in the input message are then taken.

System Relationships



The RARS Expert processes various events resulting from other input such as environmental alarms; messages received from other sources such as MSWindows and may be passed to the Expert for processing. The following standard input messages are presented to the Expert for processing when they occur.

Alarm activity

The RARS Server has an application that controls the management of alarms. Alarms are on/off conditions such as physical switches, applications running, remote host Pinger alarms

etc. The alarm manager finds these conditions in an alarm table and raises or cancels alarm conditions. These activities are presented to the Expert as an input message type *'Alarm'*.

Period time changes

The RARS Server Period Rule Manager is used to define time to the RARS Server such as business hours holidays etc. When the state of these rules changes these events are present to the expert as Type *'Period'*. The input contains fields such as the name of the period rule, which changed state and the current state of the period rule.

Message Delivery

The RARS Server Messaging application delivers messages to end users via SMS, Digital Pager, and Email etc. When the Messaging facility delivers a message or fails to deliver a message input is presented to the Expert of the type *'Delivery'*. The input contains information about the message, the target of the message and the delivery status.

Incident Processing

The RARS Server Incident application controls the processing of events which should inform standby personnel of errors which have been detected. This may be as a result of an alarm or a message received from other sources. An event filter table is scanned in an attempt to find a matching event filter. The matching event filter defines the standby personnel responsible and how they should be informed of the error. Escalation methods are defined in the standby group. Any activity taken on an incident is passed to the Expert as type *'Incident'* containing the information of the incident at that time.

System Values

The RARS Server supports a table of system values, which may be manipulated by the user. System Values have a unique name and a value. These System Values are created by the Expert, the user, or programmatically based on actions taken in the RARS Server.

When a System Value changes it is passed to all clients connected to the Server such as Graphical Viewer and to the Expert. The Expert input is of Type *'System Value'* and the fields include the name and the value of the System Value.

User Defined Expert Input

User defined Expert input types may also be created and processed. This is achieved by writing Expert Input formatted files to specified folders.

Expert Criteria Rules

All expert inputs are written as Expert Input formatted files to designated folders. Directory Scanners defined by the RARS Server custodian reads files from these folders, either to convert them to Expert Input format or process them directly if they are already in Expert Input format. The input is passed to the Expert Criteria Selection Facility which compares each input message to the Expert Criteria Rules defined by the RARS Server custodian (Administrator). If the input matches all actions defined in the matching rule are performed.

Each action, which may be performed as a result of the criteria matching for an Expert Criteria rule has information, required by the action. For example writing a file would require the target file name and the data to be written to the file.

Action information fields can be provided as literal text, information taken from input fields in the input being processed, or part thereof.

Where complex information is required the information may be formatted using an Expert Formatting Rule which concatenates multiple input fields, literal text, System Values and/or Global Variables to form the information required by action information parameters.

The actions may be one of the following:

- Write a file
- Trigger an incident to process
- Send a message using the Message Scheduler
- Send an SNMP Trap message to a selected host
- Take action on an Alarm Manager Alarm
- Set a System Value
- Trigger an Event Correlator
- Run an RARS Server script
- Execute an RARS Server command
- Launch a windows program
- Send an Email message

As the Expert operates and makes decisions on input received, the Expert Criteria rules are created by the administrator using information, which is not directly available at the time of definition. This makes the process very complex because the rules are abstractions of the input being processed. To assist the administrator in this process the Expert provides a Sample Collection Facility. When this facility is enabled in the settings of the Expert Directory Scanner each input being processed saves a copy of the input to a samples library. While defining an Expert Criteria Rule or an Expert Formatting Rule the administrator can select a sample, which would represent the input for which the rule is intended. Once the sample is selected the rule definition dialog indicates to the administrator whether the rule would match the criteria. Once rule match has been achieved the administrator may define the actions required. The action parameter fields may again be defined using the selected sample as input. A simulation facility may be used to actually execute the Expert Rule being formulated against the selected input sample. The result of the criteria match and the output of the actions are displayed to the administrator. The administrator may also elect to actually execute all the actions which would result in the actions being processed by the Expert as if the selected sample input where a real production input. Once the administrator is satisfied with the operation of the Expert Criteria Rule being defined it may be saved to the active Expert Criteria Rule Table which immediately places the rule in production. No RARS Server restart is required to enable any definitions made in the Expert.

Each Expert Criteria Rule has input fields indicating the date and administrator, who formulated the rule. When a rule is modified this information is also stored. A comment field enables the administrator to save comments and documentation together with the rule.

Graphical Viewer

Graphical Viewer clients are installed on desktop computers attached to the network and display graphically the status on all active alarms managed by the RARS server. The user can customize the views to taste with various graphical objects being available. These include images, text captions, buttons and meters. Buttons can be used to control outputs in remote nodes

A graphical representation of the status of the entire network can be displayed, highlighting problem areas immediately when they occur.

The Graphical Viewer will:

- Auto learn when new alarms are installed
- Ability to control – switch relays on/off on RAMM units
- View Alarm conditions graphically
- Viewer can set its own alarm conditions
- Display multiple external systems/ servers/ applications/ conditions online on one viewer and can be displayed on a billboard at the same time if needed
- Can define own Icons
- Icons: Analogue – Needle, Digital meter – Digital reader, thermometer all can be calibrated independently to fit unique requirements
- Handle analogue visual meters and set limits
- Display external system data / indicators

Every Viewer is handled as its own desktop, i.e. multiple Viewers can have different views.

The server provides facilities to partition the monitoring environment in such a manner that multiple enterprises can be monitored from a central site. This is achieved by definition of a departmental organigram of multiple organisations. Users accessing the system are assigned the visibility of the resources and personnel applicable to their organisation or department only. Application process views may also be shown, for example, display the servers, databases, switches etc associated with the application 'Payroll'.

Process

The monitoring of processes, executed by a single system, provides a framework for developing timelines, building teams, and defining goals and milestones. Regardless of process scope, a set of managed rules will expedite work and help ensure that all bases are covered.

An end-to-end view of all applicable processes in the service delivery mechanism is therefore vital to ensure successful service delivery.

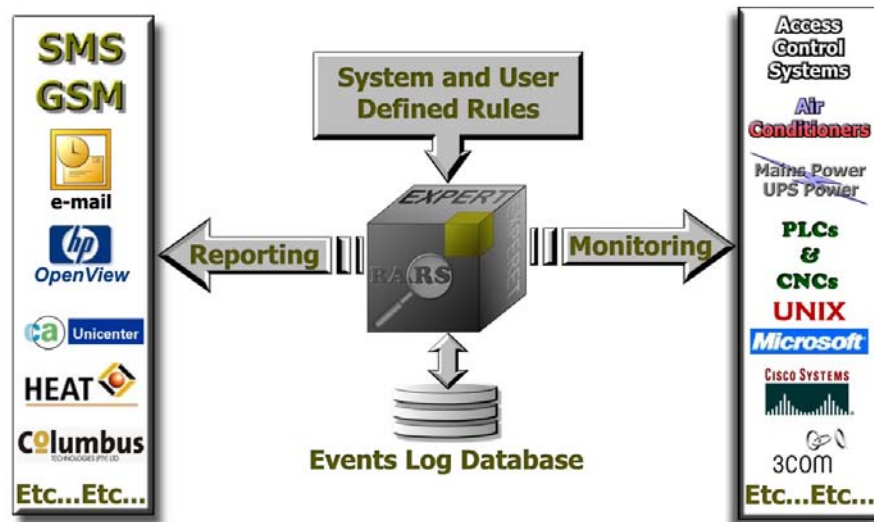
The RARS system provides powerful facilities to assist in the integration of the '*un-integratable*', and via application- and use-specific Remote Access Management Module Units (RAMM Units) we provide unattended RARS services and monitoring, no matter the location.

Using the rules-based Expert processing engine, coupled with the built-in RARS correlation facilities, we provide a vantage point from where the state of the system is displayed. A common messaging layer is created with a few point and click actions allowing for operator-less automation. Messages and alerts are forwarded to the person that was identified as being accountable for the incident, and ownership is acknowledged via bi-directional SMS

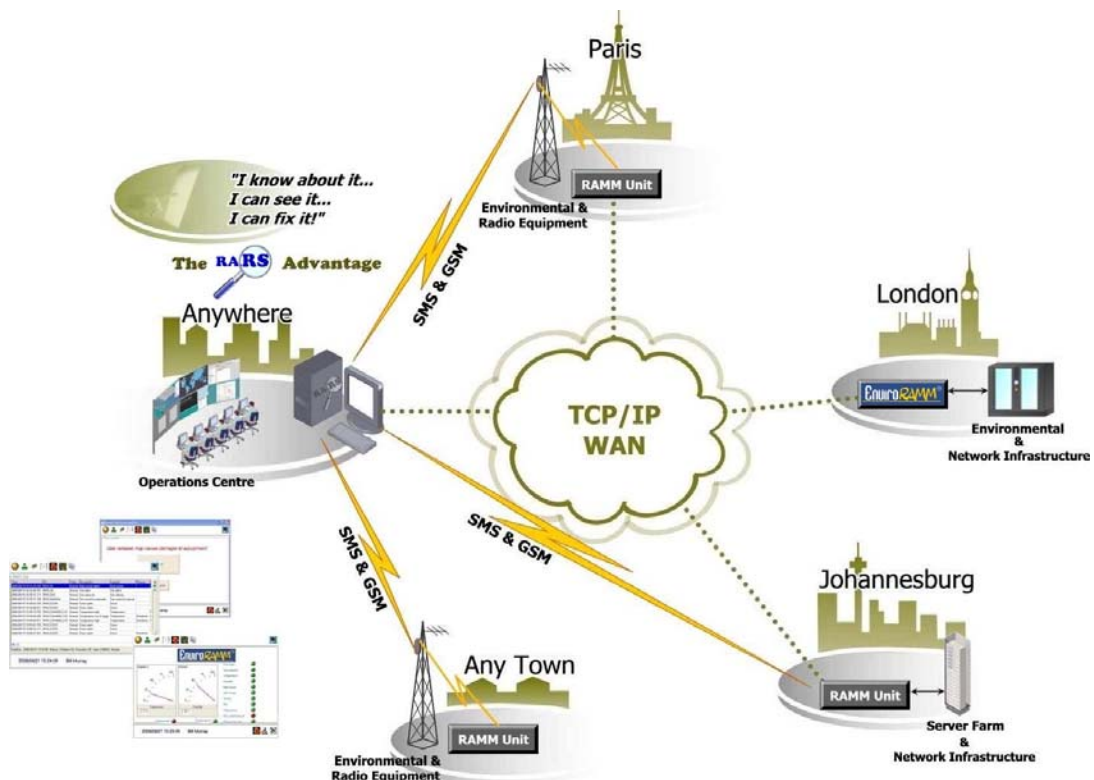
communication. Automated escalation procedures are invoked if there has not been an appropriate response within a prescribed time.

RARS has the ability to successfully measure the health, performance and integrity of the business. It checks IT systems, environmental conditions, business processes, and production systems and devices for a complete and holistic view of the enterprise that enables faster root cause analyses and problem escalation to enhance the availability of critical processes.

Using easy-to-use drag and drop facilities, we are able to distribute monitoring profiles across the enterprise in minutes and no reboot of critical devices and servers are needed if changed requirements have to be deployed.



RARS System Schematic



RARS Synopsis

Alerting

- Can send alerts in the form of e-mail
- Can optionally send alerts using SMS
- Can send alerts to multiple destinations
- Can run an action program on the monitored server
- Can run an action program on the monitoring system's server
- Can alert against a set of rules to avoid "*alert-flooding*"
- Can consume SNMP traps from other sources and send e-mail based on such a trap

Troubleshooting (Real-time graphs)

- Can chart any measured item at the measured granularity
- Can chart any measured item in real-time
- Can chart multiple measured items on one graph for correlation
- Can "*drill-down*" into causes of a spike on a chart
- Can chart multiple items on separate graphs beneath each other for correlation

Reporting (Non Real-time graphs) for trending and capacity management

- Measured data stored in a open database for reporting, specify type
- Reports granularity can be adjusted to hourly, daily, weekly or monthly
- Trend reports show a "*trend-line*"
- Can chart multiple items on one graph for correlation
- Can chart multiple items on separate graphs beneath each other for correlation
- Reports can be scheduled to run automatically, every week and/or month
- Public holidays and weekends may be excluded from scheduled reports

Reporting (Non Real-time graphs) for Service Level Management

- Service level reporting is available as part of the offered solution
- SL report can be configured for multiple levels of detail
- SL high level report is based on a single %-age of availability and performance for the environment

Completeness of Solution

- Server monitoring solution is a part of a wider solution which includes client and/or network monitoring
- Wider solution includes network element monitoring (SNMP)

Monitoring Technology

- Can use agent based technology to monitor servers
- Can use WMI to collect statistics
- Can use SNMP to collect statistics

Ease of implementation

- Can save monitoring configuration of each type of server and then roll out to all of that type
- GUI driven installation
- No scripting
- Remote agent installation utility
- Agent installation process is similar on different platforms

Ease of use

- Once installed the implementation requires minimal maintenance
- Solution has intuitive interface
- Common interface with other tools in the wider solution