

# RMU

## Remote Management Unit

Eddystone Broadcast RMU enabled FM transmitters can enable your Network Operations Centre and authenticated Engineers to remotely view and manage any transmitter system.

### Global view for global peace of mind

- Installation of the RMU box can be done in minutes and instantly start logging environmental and system parameters for remote interrogation.
- Using the RMU iPhone /Android APP authenticated engineers can remotely access and manage the enterprise of FM transmitters from anywhere they have phone signal.
- Optional KML files can be produced in near real time to provide Overlays to Google earth or similar mapping tools showing near real time Enterprise stats and warnings.
- The RMU box can be configured to collect and store system parameters, these parameters can be forwarded to a central server via SSL to enable a system wide dashboard to be viewed on the iPhone / Android or authenticated NOC Webservice.

### Modular Approach

The RMU Base comes in a 1U form factor with the ability for 2 optional modules.

Further modules can be installed into 1U RMU Expansion racks; each 1U expansion rack can hold 4 modules.

Fully configurable from any internet browser, security and authentication via LDAP, RADIUS, AD, Local internal DB.



### Connectivity

Where the existing site does not have IP connectivity onto the internet an optional GSM modem can be fitted to provide connectivity. I/O's on the rear of the units can be wired directly or bought out onto Krone punch down terminals.

# RMU

## Remote Management Unit

### Accessibility

The RMU box can be configured to collect and store system parameters, these parameters can be forwarded to a central server via SSL to enable a system wide dashboard to be viewed on a smartphone or authenticated NOC Webservice.

The Eddystone Broadcast Ltd RMU can also be configured to monitor certain parameters and if they go out of configurable limits an alert be sent to the central system (SNMP, Syslog), this can in turn send out alerts and SMS's to predefined recipients. A central system can either be hosted on the client's network or in our secure data centre hosted within Cable & Wireless High availability hosting platforms.

### Hosted System Architecture

The centrally hosted platform will constantly monitor all connected equipment, temperatures, currents, RF power, Voltages to look for symptoms that may indicate an event or even be able to pre-empt an event and alert the operators before a system event occurs. Events learnt on other systems can be matched against to provide a powerful knowledge based pre-emptive and proactive management system.

Data flows from the Connected equipment, via the RMU box and over an IP connection to the hosted platform. Data is sent over an encrypted SSL channel. Users can access the data and system information via web browsers, only after authentication with the Enterprise class Cisco Systems Adaptive Security Appliances.

### Customisable Dashboards

Either local PC or web interfaces are customisable to show various elements on the initial dashboard. Widgets are drop and drag based on connected modules. Users can then drill down into individual systems right to individual sensor, such as a temperature module or an Amp module. Reports can be exported and devices controlled.

### Multi-Site / System Monitoring

A single IRMU can poll many IP enabled devices over a LAN or WAN, this allows for monitoring of remote sites. Where remote sites require connectivity to GPIO lines we recommend installing a base RMU on site that can act as a remote agent for the master RMU.

Dashboards can be modified to show geographic map representations of the enterprise and allow the authenticated user to drill down into a particular site. These maps can be directed to a wall display for NOC usage.

