TECHNOLOGY ENABLED CARE

tec

CYMRU

Telecare Resource Centre

Device Management Systems (DMS')

December 2021

Managing Alerts

Introduction

One of the biggest changes Telecare Service Providers will notice following the transition to Digital Telecare is a significant increase in the amount of information available, particularly with regards to the statuses of deployed devices and peripheral units.

For those familiar with the use of GSM alarms this won't be anything new, as GSM units typically incorporate a device management platform (DMS), but this will now be true for all digital alarms units regardless of whether they are GSM or fixed broadband connected.

There are big advantages to this change, particularly in terms of improving service user safety. Gone will be the days of alarms being inoperable due to a faulty phoneline and the issue remaining undetected until an (unsuccessful) attempt is made to trigger the alarm.

However, there is also a risk here for telecare service providers. Having access to information brings with it the obligation to analyse and act on that information, and failure to do so could have serious consequences.

This risk can be mitigated by understanding the different alerts and having a clear policy and process for responding to them.

This document provides an introduction to some of the different kinds of alerts telecare service providers should expect to see, common ways in which this information is provided and suggests some questions to consider when developing policies and processes to manage these alerts.

Device Management Systems (DMS')

A DMS is, typically, a web-based software application created by the device manufacturer to allow digital devices to be configured, managed and monitored. As this suggests they are manufacturer specific, and so the first thing to note is that if using alarm devices from different manufacturers a telecare service will have a different DMS for each.

As well as allowing you to set-up, programme and update devices, the DMS also provides information about the status of deployed devices. There are a number of ways in which you can access this information, the ones available to you will depend on the specific DMS you are using. Some of the most common include:

Device Record

Records within a DMS are device-centric, and every system will allow you to pull up an overview of a device by entering a unique identifier such as its serial number or alarm code.

The device record will usually provide an overview of the device's status and some form of event log, allowing you to identify if there are, or have been, any issues.

However, as your typical service is using hundreds if not thousands of devices from any one manufacturer, this method is unlikely to be useful for any purpose other than checking on a specific device.

Email Reports

The most common approach to providing an update on alerts is through email reports. These can be typically configured to either send an email every time a particular kind of alert is received and/or to send a regular summary of all alerts.

A combination of immediate alerts and summaries would prevent a service from being completely overwhelmed by email alerts which don't require immediate attention and helps to highlight issues which do require immediate action.

Interactive Dashboard

Less common than email reports, some DMS' includes an interactive dashboard which allows you to specify a particular device status, for instance low battery, and return a list of all devices currently showing that status. This would remove the need for the kind of summary email listed above, and would allow for greater flexibility in how alerts are managed, as well as making it easier to identify trends and issues.

Types of Alerts

The following table lays out some of the most common types of alerts which are provided through a DMS. Terminology has been kept as clear as possible, but with the caveat that there is a little consistency in naming conventions between systems, and some have quite unintuitive names. For instance, one DMS refers to an alarm unit having a low battery as 'accumulator low', to differentiate it from the 'battery low' alert which refers to the battery on a connected peripheral device.

Alert Name	Description
Missed heartbeat	A 'heartbeat' is a signal sent between the DMS and alarm device at regular intervals (configurable by the telecare partnership) to check it is connected to the system and functioning correctly.
Low battery	Indicates an alarm unit's battery is running low.
Low battery – Peripheral	Indicates a peripheral unit's battery is running low.
Low signal	Indicates the mobile signal a GSM unit is receiving is low which could impact the success of an activation.
Radio interference	Indicates other signals have been detected on the frequency used by the unit to connect with peripheral devices.
Peripheral out of range	Indicates a peripheral device is no longer being detected by the alarm unit.
Mains failure	Indicates a device is no longer connected to the mains.
Power failure	Indicates a unit is no longer connected to the mains and its battery is running low.
No user contact	Indicates a device has not been activated within a specified time period.

Creating a process for managing alerts

Given the differences between systems each telecare service provider will need to define a bespoke approach to alerts based on the functionality of the systems they are using. The following process is suggested as a way of approaching this.

1. Determine the functionality of the DMS' being used, this should include:
    - What alerts does the system use?
    - How are alerts reported
    - To what extent can urgency be customised. For instance, can you set 3 consecutive missed heartbeats to generate an immediate email alert, but for 'no user contact' alerts to only appear in the daily summary?

2. Based on the functionality which has been identified you will then need to determine
    - How often are alerts checked and by whom
    - How quickly do the various categories of alert need to be responded to and who is responsible for responding?

3. Ensure all staff members identified in the above process have received sufficient training on the new systems and processes are in place for updating this training in line with system developments.

Challenges

This is by no means a straightforward process, and there are a number of challenges you will need to consider.

1) Devices will send status updates 24/7. You may have decided that consecutive heartbeat failures over a 6-hour period should warrant an immediate call to the service user to check-in and arrange a maintenance visit for the device, but what happens if this falls at 4am? Do you wait until business hours to avoid waking the service user and causing unnecessary panic, or do you contact them immediately to avoid the risk of them suffering an emergency and having an inoperable alarm? Does the response vary depending on the level of vulnerability of the service user?
2) If basing response on a daily report, there is a risk of potentially lengthy delays in response depending on when the criteria for action are met. For instance, suppose a process has been determined that mandates a follow up call needs to be made if a device misses a certain number of consecutive heartbeats over a fixed period. If the trigger for this is a daily report, and a device reaches the threshold 5 minutes after the daily report has been generated, that potentially adds 23 hours and 55 minutes to the response time.
3) Some DMS' send a report when an issue with an alarm is first identified, they do not necessarily send regular repeat emails to highlight that an issue still exists. It is therefore important that robust processes exist to ensure that emails are monitored and acted upon.

4) Even when operating normally it is likely that some heartbeat signals will not be correctly received by the DMS. This means there is potential for "false alarms" indicating a problem with a device. It is likely that these false alarms will be quickly cleared, when the next heartbeat signal arrives correctly at the DMS. However, the false alarm may result in an alert message/email being received by the service provider – there could be a non-trivial number of these messages received if thousands of digital devices are deployed. Service providers will need to have processes in place to monitor alerts and identify those that are likely to be a false alarm.