National Pothole Reporting System

System design

By Peter Fox, System designer

Draft version printed 21 August 2003 (8:37AM)

Contents

1 1 Overview

In this section we describe the system in general terms in order to set the scene for the details in later sections.

2 2 Functions

In this section we describe what the system does.

3 3 Database

In this section we detail the design of the database used by the system

4 4 Screens and emails

In this section we describe the web pages and how they interact with the database and each other. Also the contents of email messages.

4.1 Scope of design
4.2 Common characteristics
4.3 Public pages
4.4 HA pages
4.5 Maintainer pages
4.6 Contractors pages
4.7 System administration
4.8 Access control
4.9 Cookies

5 5 Operation

In this section we discuss how the system will be implemented and managed

5.1 Hosting
5.2 Set up and test
5.3 Training
5.4 Routine administration
5.5 System management activities
5.6 Project and quality of service delivery management

6 6 Discussion

Here we discuss some wider issues beyond technical design matters.

6.1 Success factors
6.2 Failure factors
6.3 Preparing HAs and maintainers
6.4 Measuring results
6.5 Extending the system

- ask reporters after a year if remedial action was successful

Terms and abbreviations

These terms have special and particular meanings.

Active link
: Text in an email written in the form <http://www.natpot.co.uk/......> which will appear in email clients as a button to press which when done so will launch the user's browser and take them to the appropriate page with a single click.

CA
: *Cryptic access*

Contractor
: Person or organisation which actually 'goes out with pick and shovel'

Cryptic Access
: See appendix A. A method of preventing indiscriminate access to web pages.

HA
: Highway Authority ... Body with formal responsibility for maintenance

Job
: Activity within *maintainer* related to one or more *Problems*

Locality
: An area which is used as a first approximation to classify *locations*

Location
: A small place which identifies a patch of road

Maintainer
: *HA* or a sub-contracted local authority

NFA
: No further action

Problem
: A single defect

Report
: One or more *problems*

Reporter
: Person making a *report*

1 Overview

In this section we describe the system in general terms in order to set the scene for the details in later sections.

1.1 Purpose

The primary purpose of this system is to provide a simple to use and effective method for members of the general public to report highway defects such as potholes to the bodies who are responsible for mending them.

Secondarily this system will provide:

- Feedback to reporter
- Visible progress and statistics in the public domain
- A simple and standard method for maintainers to progress problem reports

1.2 Implementation

The complete software and database will be implemented on a single web server. This will mean that the only IT requirement for the public and the maintainers is a standard web browser and access to the Internet.

When a report is made the details are placed on a database and an email notification sent to the supposed maintainer. On receipt the maintainer will carry out some investigation and possibly action and keep the database up-to date using simple web pages.

As the maintainer, reporter or third parties add items to the problem report the reporter and maintainer will be sent a copy by email and the database updated in real-time for public view.

Slight variations in protocol will be used where there are urgent reports, but in the main all communications will be via the system which will be able to apply appropriate privacy rules.

Maintainers will be able to use a job management system which allows more details of 'who should do what by when and what was the result' in a private format while still being tied to the problem report.

1.3 The reporter's view

1.3.1 Current problems

The reporter is the member of the public who has made the effort to report one or more problems. People who have tried this have a generally negative view of the current process and many simply give up and don't bother in future. The main complaints are:-

- Difficulty in getting to speak to the right person
- Lack of response from the HA/maintainer

- Inability to get accurate information about what is happening

Note: HAs need reports from the general public as surveys are rarely frequent enough, and preventive action rarely sufficient to prevent serious defects appearing. Of the few people who believe in civic duty only a small fraction will bother wasting their time twice - Therefore the process of reporting must have some reward - we presume that is in the feel-good factor outweighs the hassle factor.

1.3.2 Addressing these issues

To make the system worthwhile from the reporter's point of view we should make sure the three problems in 1.3.1 are addressed.

- Getting the report to the right office can be done by selecting an appropriate HA or maintainer. While some people will know straight away that the County Council are the people to contact the majority will have to search by town or village. [This data to be maintained by maintainers.]
- A protocol for handling problem reports will be used. This will require appropriate responses within appropriate times depending on the nature of the problem. The most obvious difference between the traditional method and this system is that progress is reported in public so that sloth and excuses are exposed to the light of public scrutiny.

1.3.3 Making a report

If the reporter is not already known to the system they are asked for basic contact details.

They pick or search for the appropriate maintainer.

They fill in a form on the screen describing one or more problems. Each problem will be specified in factual terms, location, nature, size and significance according to the urgency as assessed by the reporter. [The objectives are (1)to get an accurate location, (2)a reasonable description and (3)a feel for the risk.]

When the report is complete it is added to the database, an email sent to the maintainer with a copy to the reporter using the email address supplied. [Both these emails contain a quick access code to enable the recipients to get to the particular problems in a single step.]

1.3.4 Progress

From a reporter's point of view progress should be notified when

- The maintainer adds something to the problem record
- Some third party adds something to the problem record
- Optionally, something happens to another problem in the same area
- The watchdog timer expires for lack of action from the maintainer

The complete problem history is always available on the web pages.

Either the reporter or a third party might comment on the problem. For example what they see as an inappropriate response. These comments could usefully be categorised.

At some stage the maintainer will post 'no further action'. At which point the reporter may wish to disagree.

1.3.5 Re-raising a problem

Quite frequently a problem is fixed with a very poor quality repair. [This is an important quality indicator]. There needs to be a simple way of reviving a previously ‘case-closed’ problem.

1.3.6 Complaints

There will be occasions when the reporter or 3rd parties do not consider the HA’s response to be satisfactory. A complaint can then be raised which will be sent to an appropriate complaint address at the HA. This will then be progressed similarly to the original report.

1.3.7 Satisfaction and reoccurrence

When the HA posts NFA the original reporter or 3rd parties may have views on how well the HA performed. This will be a basic measure of satisfaction.

It is quite often that repairs prove less than permanent. In this case we would expect the matter to be resuscitated.

1.3.7 Notes

- People should not be using this for obstructions which go beyond a defect to say a tree across the road or actual subsidence which clearly require traffic management by the police.
- When entering problems the database will be searched for recent reports in the vicinity. The object of this is to try to avoid duplicate problem reports for the same defect. [This will happen but the HA can collapse duplicates on receipt.]
- Normally reporter’s details will be limited to name and email address.
- The risk assessment will be structured so that it can be passed to the HA as a definite quantity.
- For many people reporting a pothole or other defect is a matter of complaining about the Council’s neglect. Fury and frustration may not be the most positive reasons for reporting potholes but it beats nothing. If someone who has waited weeks eventually uses this system and gets a positive or at least measured outcome then perhaps we will have recruited another pair of eyes that will spot defects before they get to such a state in the future.

1.4 The HA’s and maintainer’s view

1.4.1 HA -v- maintainer

Many HAs operate a policy of sub-contracting road repairs to district councils or road maintenance companies. However this is a convenience arrangement for the HA who still have the responsibility. Bearing in mind the HA is accountable and an easier area to specify [fewer borderline cases] the obvious approach is to pass all reports to the HA and let them parcel out the work according to whatever scheme they operate.

However in the interests of cutting out the middle-man there is an argument for directing reports to maintainers in the first instance with the HA being the ultimately responsible body.

Therefore we propose to allow HAs to specify maintainers that reporters are asked to contact in the first instance. This give flexibility. It is up to reporters to decide if the matter should be brought immediately to the attention of the responsible HA or just to 'call out the road menders'.

Complaints about lack of action would be directed to the HA as a matter of course.

The HA would be responsible for maintaining the list of their sub-contractors and defining the areas which they cover.

1.4.2 HA's view

For the purpose of this discussion we will consider the office dealing with reports, initiating investigations and actions and updating the status of the problem.

The office will receive email notification of a report with all details. Included in the email will be a 'follow this link' to update this problem. If more than one problem appears on one report each will be given separate identification numbers. There will be an email serial number which is consecutive for each HA.

Normally the reporter will only be known by name, the exception being highest risks where a telephone number is demanded from them. The object of this is to stop the system being bypassed and thus keep all action/inaction in the public gaze.

Upon receipt the HA will be expected to prioritise investigation/action and respond according to the risk assessment of the reporter. For example the protocol may specify a 12 hour investigation response time for a 'level 2' risk.

The HA may elect to

- Request better information.
- Acknowledge with promise of investigation by a date.
- Collapse this problem with what is clearly the same one previously reported.

- Pass the report onto another HA if it appears to be a boundary error.(NFA)
- Reply that this isn't a highways matter(NFA) [Where utilities have left the road in a poor state this definitely is for the HA to sort out - It is really just a choice of which contractors the HA choses to get to fix the problem.]
- Get on with investigation/action without responding immediately.

In the first four cases appropriate database updates and emails will be generated by accessing the web pages shown in the notification email.

If there is fieldwork to be done then the HA has the option of using the built-in job recording system to pass 'investigate&report' and 'fix' instructions amongst themselves and sub-contractors. This simple job record is private to the HA/contractors but linked to one or more problems thus saving a great deal of paper shuffling.

The HA can add to the problem record at any time by (a) keying in the problem ID (b) clicking directly on a reference embedded in an email (c) selecting from the outstanding list of problems.

At some stage the HA will determine that the job has been done and will mark it NFA. [This may not be the end of the matter, the reporter or 3rd parties may consider the action inadequate.]

1.5 The public view

1.5.1 Importance

It is important that the public can view how reports are dealt with. One of the reasons for high levels of dissatisfaction is poor service resulting from knowing that a slothful and self-serving organisation can almost always ignore an individual.

If poor local performance is evident then local people have councillors to harass in an attempt to get the, plainly documented, problems addressed. This is a two-level thing: (1)'Fix the hole' and (2) Fix the system.

Therefore it is important for people to be able to list outcomes and still-outstanding matters with levels of satisfaction and factual data regarding what happened when. Typically this would relate to one or a few reports in a particular locality.

If an accident occurs then there is immediately evidence that the HA knew about the problem, and are potentially liable for damages. The status and history of a locality can now be obtained by a quick search including for the first time having confidence in being able to access information if it exists.

1.5.2 Local knowledge

Some potholes are so large everyone assumes somebody knows about it. Clairvoyance is definitely not on the list of skills possessed by HAs! Therefore a quick check on the web to see if anyone has reported it is called for:

- If nobody has reported it then I will.
- If it has been reported then why the hell is it still left like that?

Therefore being able to search recent problems by street name and locality is required.

1.5.3 Performance statistics

There are some opportunities to measure speed of response to different levels of urgency and risk, public satisfaction and recurrence levels. Not only does this provide an opportunity for HAs to be measured but they in turn will be able to compare the performance of their sub-contracting maintainers.

1.6 Making the system successful

This system depends on being used by the public. Publicity will be required to get this started.

Public participation is entirely voluntary so a poor public image, difficult interface and continuing frustration with slothful and patronising HAs will mean it withers. On the other hand if it delivers its promises then people will use it again and recommend it.

There is an element of 'have-your-say' in this system with reporters being asked how well they think the HA has dealt with the issue. This is important because the small proportion of the general public who can be bothered to report defects are typically 'vocal-locals' who don't expect to be simply milked.

2 Functions

In this section we describe what the system does.

2.1 Making a report

Note that the following order of description is not a preferred order of flow and should not be used as a template. It will become apparent that these interlinked matters could be presented to the reporter in different ways to give a smoother and more reliable process.

2.1.1 Identifying the reporter

We need to know who the reporter is so that they can be mailed by the system. Note that we do not normally pass on contact details to the maintainers. The main reason for this is to stop maintainers bypassing the system.

Web browsers can store a user's details on their own computer.[Using 'cookies']. This means that a typical user does not have to keep re-identifying themselves manually, instead the web page[server] asks the web browser[client] if this is a repeat visit and if so could it pass the reporter's ID across so it can look it up in the list of reporters.

The information asked for would be

Ordinary name	Eg Mary Smith
Role	Eg Clerk to Littleton parish council
Email address	Must be valid
Telephone number	Only required if urgent problems are being reported.
Tell me if there are defects being NFAed in these locations	Optional list of villages or streets
Postcode	Optional

This would be accompanied by a clear statement of how far the data would be spread. In particular:

Email address - Not passed on to anyone
Telephone number - Only passed to HA for urgent problems
Postcode - Not passed on. May be used for statistical analysis

All of these can be modified at a later date.

2.1.2 Identifying the HA

This is quite a tricky operation because it is not always obvious which is the right HA/maintainer.

The correct maintainer might change from one side of a bridge to the other or two ends of a country lane may have different maintainers. Therefore this is never going to be perfect. [Hence the facility for a HA to forward the problem on receipt.]

a

Major trunk roads are maintained by the Highways Agency. We should be filtering these out if possible. One way is to ask for an 'A' road number and look up a database of A-roads which the Highways Agency maintains and return matches with descriptions for ticking.

b

Many people will be able to make a good stab at the appropriate HA, typically a county council or city council. In this case typing in, or selecting say 'Essex' will bring up a list of places covered and possibly a list of sub-contracted maintainers.

c

Many people will be concerned with the same small area and maintainer for subsequent reports. Therefore it makes sense to keep this as a cookie or on the reporter's record for convenience.

d

Why not defer determination of HA until 2.1.3? This is fine when firstly it isn't a trunk road maintained by the Highways Agency, and secondly that the place isn't in the middle of nowhere.

This a,b,c,d list can be converted into a four-way form from which people can use the method that looks easiest.

Method d would involve a search on the list of places [There are roughly 25,000 in England, Wales and Scotland] and return a list of possible places along the lines of

Brocklebank (Dorset) CC
Lit. Brocklebank (Dorset) Wareham BC
Brocklebank Castle (Lincs) CC

A complicating factor is that multiple problems may be the responsibility of more than one maintainer. This means that the reporter may have to come back to this screen to start a fresh report. It also means that we should be trying to validate places against maintainers as we go along.

2.1.3 Describing a location

Experience shows that it is far more difficult than one might expect to describe the location of road defects in a way that maintainers can understand. A map reference doesn't appeal to maintainer's at all even though this may be the most appropriate method in rural areas. The geographical faculties of many reporters are often rather vague. Obviously we need to do our best to make this a reliable operation.

We need to allow for the case where the defect is "between A and B" and therefore should have multiple selection opportunities.

There are various possibilities:-

a

Drill-down by map scale. This can be time consuming when most reporters already know the detail. However as there are already web resources which allow this perhaps we should provide links for those who like this method and get the reporter to input the resulting map reference and/or street name. Re-implementing such functionality in this system seems a bit excessive.

b

Pick from a list of places. A straightforward scheme where places are matched with maintainers. This would be the same mechanism as used in 2.1.2.d above.

c

After a or b, a street, landmark, distance-from, junction or other factual locator. In built-up areas many streets have numbered lampposts. This would be a descriptive field, for which we would have to give good guidance as to what is useful.

d

Map reference

Getting a good location description is quite difficult in the countryside. (In towns and villages the streets are short and there are house numbers and identifiable buildings.) Bearing in mind how useless a report is without a good location we may need to give extra hand-holding on the input screen to coax a reliable description. It may be a good idea to ask the reporter if the location is difficult to describe if they would supply their telephone number. For example, if the location is more than 200 yds from any clearly identifiable place.

2.1.4 Trying to avoid duplicates

Duplicate problems for the same physical defect serve no purpose and cause more work. That doesn't mean though that people should shut-up just because there is an existing report - Possibly the problem has got worse, or local feeling is running high, or a repair has proved to be inadequate.

So we want to encourage people to join in on an existing problem rather than muddying the waters with a phantom. The obvious way is to display a list of recent problems, both ongoing and NFA, in the locality. There are three benefits from this:

- Quicker location for the reporter
- The reporter can see the current problem status
- Avoiding duplicates

To make this effective we want to make the local defect list available before the reporter slogs through the process of making a separate report.

The implication is that the database must be capable of identifying problems by locality. Remembering that locality can be a place name picked from a list this makes it reasonably easy for a database to pick out. (Note that *Location*, being an ad-hoc descriptive, as opposed to a categorised, term is unlikely to be much use in this respect.)

2.1.5 Describing a problem

There are two aspects to describing a problem

- Physical characteristics
- Hazard

a Physical characteristics

We are not limited to potholes, there could be problems with signs, street lights, bank slips, overgrowth, blocked drains, street works, slippery surfaces at roundabouts, melted tar, blockages on RUPPS and so on. Yet while allowing reporters freedom to describe the real world as it really is, we also want a little bit of discipline just so that pertinent features are presented to the maintainers quickly and unambiguously.

Here are some actual examples of ‘potholes’

- Groove along road which could have a tramline effect on cycles. Insignificant by motor vehicle standards.
- Sunken manholes
- Hole at edge of drain or manhole
- Road surface beginning to break up - will need attention before it becomes a real hole
- Generally terrible road surface
- Ruts hidden by long grass in RUPP
- Holes just skimmed over while resurfacing without being filled-in first

From this list it is clear that there cannot be a complete classification system.

Experience shows that maintainers are not very good at dealing with the words the public use to describe defects and have a habit of failing to use their initiative when looking for a “manhole” which they see as a “hydrant cover”. This system can’t address this issue except that if nothing happens people will soon get to know about it.

The public doesn’t have tape measures and surveying instruments so there are limits on the accuracy of problem reports. “About the size of a dinner plate 1/4 mile past the old farm shop” is the best that can reasonably be expected.

b Hazard

Most people making reports are keen to see council resources used appropriately and have no problem with a maintainer taking longer over less urgent matters - providing they are not forgotten. The other side of this coin is that where there is an imminent risk it should be dealt with promptly. The public are not all stupid and some are experts so it is reasonable for them to indicate the degree of urgency which they feel is appropriate. We suggest the following classification.

- Accident has happened
- Serious danger - imminent risk - may need warning signs
- Unsafe - problem should be investigated promptly
- Needs attention - Below acceptable standard or soon will be

Then we ask the reporter to describe the risk in everyday terms. eg “Blocked drain overflowing will freeze into an ice rink”

The way problem reports are investigated will depend on a protocol. This will specify the appropriate actions and time-scales for investigation etc. [If the HA has a different view of the risk then this will trigger a reply to the reporter.]

c Making sure the problem is suitable for reporting

There are three cases where we do not want this channel to be used (or not to be the only one)

- Police matters - Where warning signs or immediate action is essential
- Burst water mains etc - Where it is better to report direct to the utility
- Planning and design - Not maintenance

There are bound to be grey areas. For example a sore point with local people is bound to be reported many times even if it really needs a policy decision to resolve properly. A collapsed manhole is probably a matter for the police, the HA and a utility - but expecting a member of the public to sort out which particular utility is too much to expect.

Therefore we need to provide:

- Clear instructions about what this system can do and who to contact otherwise
- Each HA should provide a telephone alternative ‘highways hotline’, where at least if it is not continuously manned the answering machine will give an indication of when it will be dealt with.

d Photographs and diagrams

The object of this exercise is to give the maintainer enough information for them to know what sort of defect they are being asked to investigate in order that the appropriate resource may be allocated to that task. Whilst a reporter may have taken photographs these are unlikely to add further useful information. (This isn’t to say that reporters should not make their own records - It may be quite important for them to do so where they do not trust the HA to deal with the job properly, have an accident claim, or want to show evidence of long-term neglect.) Therefore it can’t really be justified to provide the added complication of a method of attaching binaries.

Some people think a diagram is needed, but the time taken to draw it is likely to be much more than the same amount of care put into a description in words.

2.1.6 Updating the database

This should be a straightforward matter. This must be done before the emails in 2.1.7 are sent.

Each problem will be given a unique ID.

Although a reporter may put multiple problems onto a single report we do not see the need to have a separate database table for logging reports as this information is not going to be used later. During the creation of the report we want to batch the problems together for convenience so we may deal with them in single emails as in 2.1.7 but after that each problem stands on its own.

In addition to updating the real database we may want to update the cookies on the reporter’s browser with HA,problem ID

2.1.7 Sending notification emails

One of the key aspects to this system is that reporters and HAs do not normally email each other directly. Emails (as opposed to web page information) are needed because of the active notification aspect.

Note: Emails sent by the system are not meant to be replied to by email. The only correct reply method is to use the embedded links. Therefore when the system sends an email we set the 'reply-to' to the recipient so that if they try to reply by email it just gets returned to themselves and puzzling them rather than going on a trip into the unknown.

a Email to maintainer

HAs will be responsible for ensuring a suitable email address is provided for initial reports. This may of course involve checking that he email addresses of the maintainers are correct. The protocol will set out how this email address is to be 'manned'.

For neatness multiple reports to the same maintainer will be bundled into a single email.

The details for each problem as obtained in 2.1.3 and 2.1.5 will be listed in plain text.

Urgent and difficult to locate problems will have the name and telephone number of the reporter listed, otherwise just the reporter's name.

Embedded in the text will elements which most email clients can present as active URLs in the form <http://www.....> which point to web pages. These can include enough information to take the reader directly to the problem in question. So the link might look something like this:
<http://www.natpot.org.uk/problems.php?pid=12345&mid=A0F6D7&act=ir>

These active links will need to be clarified at the detailed design stage.

b Email to reporter

One of the problems with on-line systems is that the originator often doesn't get a copy for their own records. We solve this problem by sending almost a 'bcc' back to the reporter. This also contains what happens next and embedded links for following up.

c Copies?

Reporters who feel that whatever action is taken by the maintainers will be too little too late may want to post to local councils or councillors. Sometimes this is the only way to get any action. So should we incorporate a 'tell also' facility? We think not. As the reporter has a copy of their report sent back to them by email they can forward that with the appropriate covering note tailored to the recipient if they wish. This will probably be more effective anyway, coming from a real person rather than a robot.

2.1.8 Notes

a Privacy

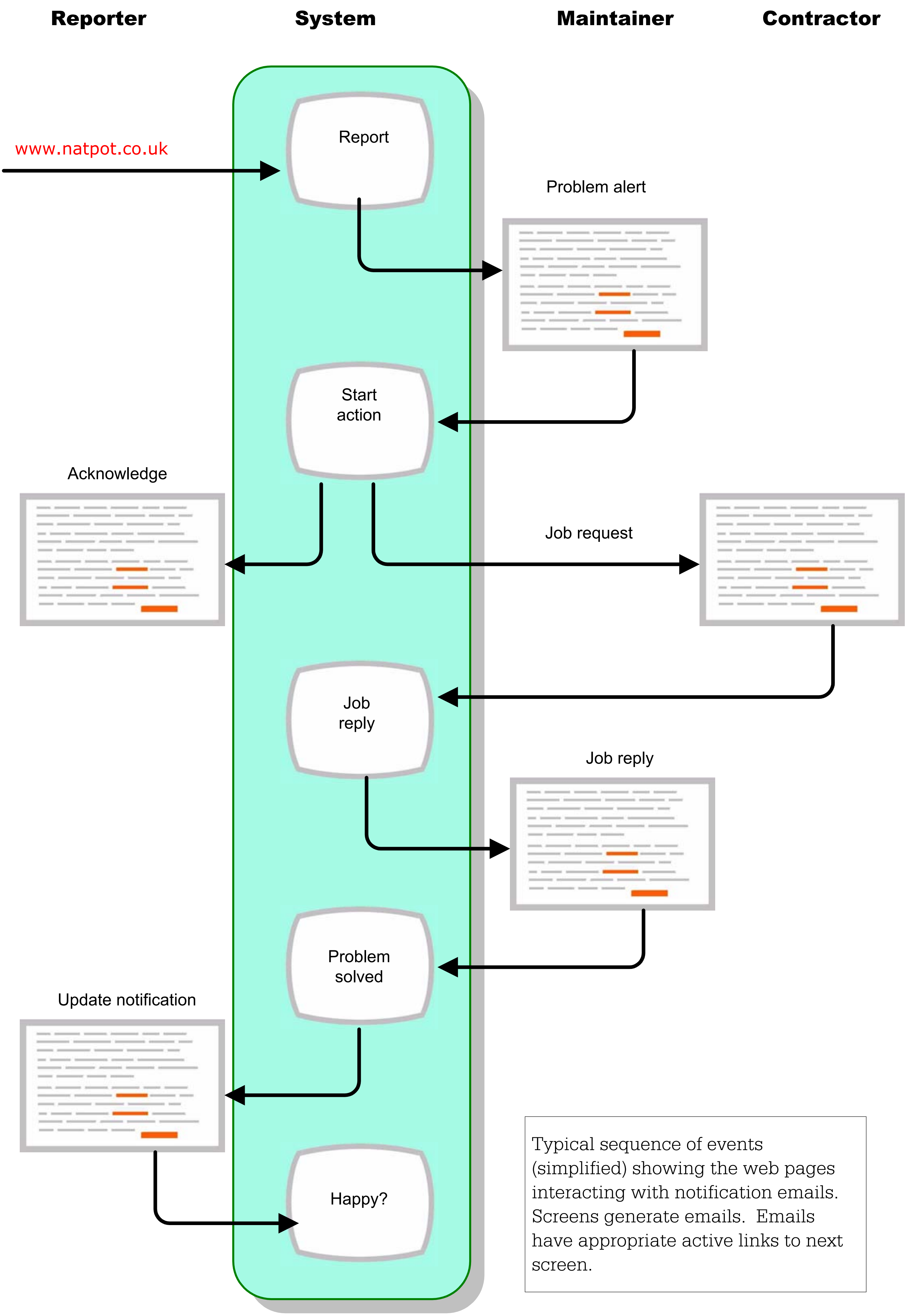
We see no need to keep information about reporters other than to facilitate efficient communication.

There is no intention of passing postal addresses to HAs, in fact we don't collect them in the first place.

We may use the postcode to perform statistical research. Although there is no definite proposal as to the nature of this analysis there would be no connection with individuals.

b Abuse

It would be possible for a person to make many reports about the same thing or a purely imaginary thing. We may need a procedure to blacklist email and machine IP addresses. This issue should be the subject of debate in the light of practical experience.



Typical sequence of events (simplified) showing the web pages interacting with notification emails. Screens generate emails. Emails have appropriate active links to next screen.

2.2 HA responds to problems

The way HAs and maintainers respond to problems in general, the time-scales and appropriate actions are described in the protocol. Here we are concerned with giving them the tools to carry out the job rather than the rules under which they ought to be operating.

2.2.1 Overview

HAs and maintainers have two points of contact with the system. Receipt of emails and browsing web pages. Emails are used for notification and carry with them the embedded links to jump to the relevant web pages. As all emails should be being passed through the system there should be no need to type in information that is already known.

The maintainer's view is on two levels of detail:

- Problems - the same as reporters and the public
- Jobs - A private (and optional) task management system which can deal with the detail of allocating work while being linked to the problem.

For example the problem "No123456 - Potholes at Jct. School La./Mill lane" might have a job attached looking something like

12/03/04 11:03 Mary to Charlie : Pls. Have a look at this today
12/03/04 15:33 Charlie to Mary : Marked for patch. Priority 2.
12/03/04 16:11 Mary to Bitumen xpress Ltd. : Add to this week's patch list
12/03/04 16:11 Mary sets watchdog - 7 days
12/03/04 16:12 Mary to NatPot : Scheduled for fix this week - Thanks for telling us
18/03/04 13:45 Bitumen xpress Ltd. to Mary : Patched
18/03/04 15:22 Mary to NatPot : Contractor reports fixed. (NFA)

This might seem a lot of hoops to go through but really it is only a record of the necessary communications. Furthermore the system is efficient because it is completely electronic with all the necessary email and web addresses available at a click.

2.2.2 Initial receipt and response to problem notification email

On initial receipt of problem notification email there is a basic evaluation process:

a Is this in our area?

There are bound to be problem reports which are not the HA/maintainer's area. (This arises because of the difficulty of specifying exactly the boundaries of maintainers.) Therefore incorporated into the email will be a set of links which require

- two clicks to forward to the neighbouring areas
- a click to get to an area search/select page
- two clicks to respond with a "Sorry, never heard of this place" message

b Is this a duplicate?

Although by the design of the user interface we have encouraged people to join an existing problem rather than start afresh there may still be duplicates which ought to be folded into an existing problem. This isn't quite straightforward because similar doesn't mean identical. Perhaps a reporter has seen one defect being looked at and thinks the HA ought to look at this other one while they're at it.

How to present just enough information to make a judgement? We might list in the email all the defects for the last three months (poor repairs being a major issue) in the locality. However this could easily result in too much information which isn't scanned as a result. Or we could leave it to the vague recollection of the person who deals with these reports to jump onto the appropriate web page and search the same list - but probably with similar results. What we might be able to do is look for similar words in the *location* field for recent problems in the same *locality*. This may need some tuning, but could be an effective filter.

Therefore we intend to include possible matches as filtered by artificial intelligence in the notification email with a two click procedure for merging and responding to the reporter. Also we give a single click access to a more general web page listing of defects in the locality with variable search parameters.

This would cover on-going issues where a previous response and history will be sent to the reporter thus saving re-typing the problem status report.

c What track do we send it down?

Having established this is a real problem that the maintainer has responsibility for, the action to take depends on the nature of the problem as moderated by the protocol. Possibilities (in combination if necessary) are:

- Right area but wrong department. eg. a planning matter.
- Pass on to utility company (and set watchdog)
- Get more information from reporter (possibly by telephone)
- Acknowledge and promise action by a certain date (Thanks and NFA) For example a defective street light problem hardly warrants investigation and multiple progress messages. This should be a purely routine matter of notifying the lighting contractor.
- Acknowledge and promise further reply by a given date
- Instigate site investigation (and set watchdog)
- Instigate safety measures
- Instigate repair (and set watchdog)
- Add to low priority list (and set watchdog)

(A watchdog is a sort of alarm clock which triggers after a specified time.)

These options would be selected from a single web page accessed by a single click. That would then lead the user through any additional stages.

2.2.3 Using the job system

a About the job system

The job system is optional and available to maintainers who wish to use it. (It is of course hosted by the web server with no local software required.)

It combines three things in an internal record

- Simple to use message passing
- Recording these messages in a log
- Watchdogs to spot no action after a given time

The same paradigm of work on a web page to trigger the appropriate emails which then have embedded links to work on a web page is used.

For the purposes of HAs and maintainers the job is connected to the problem. One job may be connected to many problems.

HAs are able to access the job records of their sub-contracting maintainers. (The reason for this is that if the problem is not resolved by a sub-contracting maintainer it will be escalated to HA level who have the legal responsibility.)

Jobs have job-items. These are the 'please do this' and 'done that' orders and replies. A job item may have a 'do by' date which if there isn't a reply will set off a watchdog timer which sends a notification email to the originator.

More details of the ancillary data associated with a job such as cost codes, and the convenience aspects such as bank of regular contacts is given in section 3.

b Adding a 'please do this' job item

The details of setting up a new job have yet to be detailed. We assume for now that a minimum of standing information will be put into the job header such as the initials of the person starting it and perhaps a cost code. Most of this information could be stored locally using cookies.

Let us assume that on receipt of a problem the person fielding it decided to pass it to someone in the field for them to investigate.

- Click on link embedded in email goes to web page
- Tick 'new job' and finish off any new job details
- Select person to send message to from list of regulars
- Confirm initials or name of sender
- Type in request
- Set a number of days allowed for response
- Click on 'send'.

This will

- send an email to the selected person with an embedded link for replying. This will contain the problem details as well as the bare message.
- make a record of message, date and time and sender
- set up the watchdog
- (in the case of initial response) send a 'we'll get back to you within X days' email to the reporter and add that message to the problem log.

c Reporting back on the job item

When the task has been done the recipient can look at their original email message then follow the link to reply with whatever message they wish.

Also contained in all such messages is a link to a list of recent requests and replies. This is bookmarkable so that somebody who tends to receive task requests can quickly access their page of tasks and reply that way instead.

2.2.4 Overview of problem status progression

a Minimal reply

A normal problem would typically involve some reply back to the reporter - Perhaps just "Thanks. We've had a look and will fix it in the next 7 days" and NFA. This, and more involved status reports are collected into a problem log which is then available on-line.

b All join in with status reports and observations

While this rosy picture of ‘Monday morning : problem reported - Monday afternoon : everything in progress’ may be true in many cases there will be a large number where things are not sorted out smoothly, in a proper time-frame, or the same problem is revived because of poor remedial action. Now the problem log gives a complete history of the problem, promises, excuses, claims and opinions. This log is open to

- Maintainers
- Reporter
- Third parties

So for example Mr. Smith might point out that the repair to the problem originally reported by Mrs. Jones failed to take into account the similar hole 10 yards up the road. Or Mrs. Brown might add to a problem reported by Mr. Black concerning vegetation cutting that round the corner ought to be done at the same time.

Third parties would normally have to drill-down through web page searches to problems in their locality, but the reporter and maintainer will have active links in their email correspondence which will take them directly to the appropriate web page.

c Tapping local knowledge

We propose to give people the ability to request email notification of new problems in a locality. The reason for this is, as in the Mrs. Brown/Mr. Black example above, that local knowledge may be very handy in being able to kill two birds with one stone with obvious savings in effort. It is easy to imagine Mrs. Brown being the parish clerk, or secretary of the cycling club.

d No further action

The maintainer can post NFA to the problem log.

Of course this may not be the real end of the story, it may even be the starting-gun for a complaint that the roads are not being properly maintained. Once NFA has been posted the ball is back in the reporter’s court if they think that more needs to be done.

The posting of NFA triggers an email to the reporter which includes

- Problem log
- How to follow up if dissatisfied

e Dissatisfaction

Once NFA has been posted the reporter has the ability to cause emails to be sent to the HA’s complaint email address. (Or the parent HA of the maintainer.) Simply a ‘why are you unsatisfied?’ web page which when submitted goes to the complaint email address with a summary of the problem log. This email would have active links to the problem and to the job (if any).

2.2.5 Notes

a Security

While there is nothing very sensitive held on the system there could be an issue if a contractor causes imaginary work to be put into the system. For this they would have to either pose as reporters and report non-existent holes which they then get paid to repair, or use the maintainer’s authority to inflate job tasks.

In addition to normal auditing procedures the following security measures can be used:

- An imaginary problem may be spotted and queried by members of the public who have asked to be notified of problems in their locality.
- Providing authenticated log-in for maintainers
- Ensuring jobs and job items are indelible and serialised
- Statistical report of who job tasks were allocated to
- Statistical/exception report of which IP address was used to allocate jobs. (This may highlight an authorised council employee using say a home computer to do a little bit of work on the side.)
- Although access to maintainer's web pages will be authenticated, we will also perturb the page modifiers (ie the bits after the page reference following the '?' such as the maintainer's ID) just to be one more obstacle for idle hackers. So instead of say "?mantid=123+jobid=456" we might use a more sophisticated version of "?pageref=654321".

b Could the job system be used in standalone mode?

This might be something to look into as a future development. As the system is designed at the moment only problems which are reported by the public can use the job system.

One way to deal with this might be to allow HA staff who come across problems by other means (perhaps they receive a phone call) to type in a report themselves. There is no reason why they shouldn't although some of the mailing backwards and forwards could be cut-out.

2.3 Further responses and counter responses and observations on problem

This has mostly been covered in 2.2.4.

a Escalation

Whilst normally a reporter should wait until NFA is posted by the maintainer, there may be cases where the reporter feels that the process is, say, dragging on for too long without a conclusion. In this case they should be able to send a complaint to the HA's complaint email address.

At this stage we still want communications to be via the system so we keep to our active links to web pages in emails paradigm. Really all we have done is to get another party involved. Their contributions get added to the problem log in the standard fashion.

b Further escalation

At this point the parties have probably reached an impasse which will involve people who are unknown to the system. Therefore communications will have to be carried out using other means. We think it quite likely that an aggrieved reporter would post a comment on the problem log so that others can see what is going on.

2.4 Maintainer's job management

A lot of this has been described in section 2.2.3.

To summarise:
Maintainers will build up a contact list of the people they use to investigate and repair. This will then be a convenient pick-list.

When viewing a problem they will also see the job history.

Maintainers will also be able to see all outstanding job items in date, locality, or person/contractor dealing with it order.

People dealing with job items will be able to see a list of outstanding and recent job items in date, locality, maintainer or maintainer reference order. Note: It may be the case that say the contractor who looks after streetlights does so for more than one maintainer. This isn't a problem as each job item 'knows' who created it - In fact it is a bonus as there is only a single interface for multiple maintainers. The 'maintainer reference' will probably be a general order number or cost code used when asking this contractor or person to do the job.

2.5 Making data available to the public

2.5.1 General principle

It is an important part of this system that anyone can see what is going on in order to counteract the unfortunate tendency of councils to be judge and jury on their own work with the consequence that standards can easily fall well below what the public expects.

The other side of this coin is that the public, should they be interested, can see the explanation for why a problem cannot be fixed overnight and perhaps appreciate that maintaining the roads is more complicated than waving a magic wand.

There may be cases where an accident has happened and the state of the road may be thought to be relevant. In this case a search for what information the HA had and what warnings were given to them by reporters may be very important factual information.

2.5.2 Problems in locality

Most people will be interested only in their locality. They know the names of the places and can search/select for their town or village.

A few people may have difficulty identifying the locality by name, particularly in rural areas. We suggest that if they are really interested they will get near to the place then telephone the relevant maintainer as given by the index of locations. For convenience we can direct them to outside mapping resources as described in 2.1.3.a.

Therefore we propose a problem listing screen showing problems for a locality. The extend of this list might be set by default to show a summary of say the most recent 40 problems with options to change the number to show and possibly a key word to filter on.

This list would lead onto the problem details.

2.5.3 Problem notification

There are some people who take a civic interest in seeing that the county council is on the ball. Also some people tend to get pestered by the public about this sort of thing - Parish clerks for instance. Therefore we propose a mechanism for people to request an email notification of when a problem in a locality is first reported, leaving it up to them to follow it up in more detail if they want to. See 2.2.4.c for discussion of the benefits to the maintainers.

2.5.4 Statistics for the general public

The 'dreadful state of the roads' is something that a lot of people moan about. We can give them some guide to the amount of activity and how promptly it was done and how satisfied reporters were and what percentage of repairs needed redoing in less than a year and so on.

The precise statistics and presentation will need to be evolved so that a fair picture is given with meaningful analysis. League tables are a simple to understand and powerful prompt for pull-your-socks-up action if the figures used are comparable and reliable.

There is no need to generate these in real time, perhaps three-monthly will be adequate.

2.5.5 Performance monitoring data

a Management statistics

Whilst the general public want to get a feel for how competent the council is at maintaining the roads, management and government like hard statistics from which to make their own analysis after concatenating with other sources of data.

One important caveat must be made. This system will only deal with reports from the general public. There is much mainteinance work which will not come under this heading. So statistics this system provides will tend to be related to public satisfaction measures rather than quantity of work measures.

Remember also that a higher than average number of problem reports does not necessarily mean the roads are dreadful or the public are unhappy about how the HA fixes the problem once they are told about it. For example a publicity campaign may save a lot of random inspections but generate a lot of stitch-in-time-saves-nine reports.

b Auditing and exceptions

We cannot say at this stage what comparative information would be useful to auditors. We suspect that interest will focus on how problems are converted into jobs. This is probably going to be a spectrum from fraud watching to more efficient working practices.

2.6 Keeping maintainers and HA data up to date

2.6.1 Principle of looking after one own's data

It is a fundamental principle of efficiency that the originators of data are responsible for recording it and maintaining it. (There is no point in somebody filling in a paper form that somebody else is simply going to type in.) Therefore once we have established who the HAs are we expect them to identify the maintainers they may use and between them and their maintainers try to sort out the boundaries of localities.

2.6.2 List of HAs

This needs to be obtained from the DfT and then loaded into the database. The complete data specification is given in section 3.

There will be gaps in this base data, for example the email address for reports. Once the system has an email address for a HA it could be operational. It is up to the HA in order to make its own operations efficient to maintain this address and to carve up its area by locality into sectors to which it wishes sub-contracted maintainers to operate in.

A web form will be provided to maintain this data.

2.6.3 Maintainers

HAs will specify their maintainers and the localities they cover.

A web form will be provided to maintain this data.

2.6.4 Localities

Initially we expect to populate the list of localities using a gazetteer and making a guess as to the responsible HA. This allocation will not be perfect but can be tuned by HAs.

It is up to HAs if they want to allocate sub-sections to sub-contracted maintainers. The list of localities can then be ticked-off into these sub sections.

A web form will be provided to maintain the allocation of localities and to add and alter localities.

2.6.5 Contacts for jobs

These will be remembered the first time they are used and then be available for re-use. In this way the contractors or units used regularly will be available at a single click.

2.6.7 Neighbouring areas

For convenience the system will remember who it went to when a problem is passed over the border, so that the next time a likely list of neighbours will be ready to select from.

2.7 System management functions

This is a low overhead system with very little central intervention.

2.7.1 Passwords and logins

The only people needing *to be given* passwords for authorisation are HAs.

It is then up to them to alter their own passwords according to their own security policies and to control passwords for their maintainers.

A facility will be provided for the system administrator to resetting a HAs password on request - subject to a security procedure.

2.7.2 Periodic activities

a Weeding

The extent of weeding is probably a matter of waiting until database performance starts to suffer and then archiving old problems and jobs

b Statistical analyses

This would not be done more often than monthly.

Some system statistics may be obtained on a daily or weekly basis to measure the load. However this information is probably best sent to a daily summary log file for later analysis as required.

A menu page for activating these analyses will be provided with the details to be developed by experience after discussion with users.

2.7.3 Exceptions and alerts

Some thought and experiment is required to spot abuse or problems. For example we might see a large number of reports for a single locality in a very short time which might indicate abuse.

We would like to install some monitor which triggers when the system becomes slow or stops so that whatever technical measures that are necessary can be put into action straight away.

3 Database

In this section we detail the design of the database used by the system

3.1 Overview

The database would be a relational database with a SQL interface. Practically all activities will be standardised queries and simple updates. There is no requirement to support ad-hoc queries.

3.2 Table specification

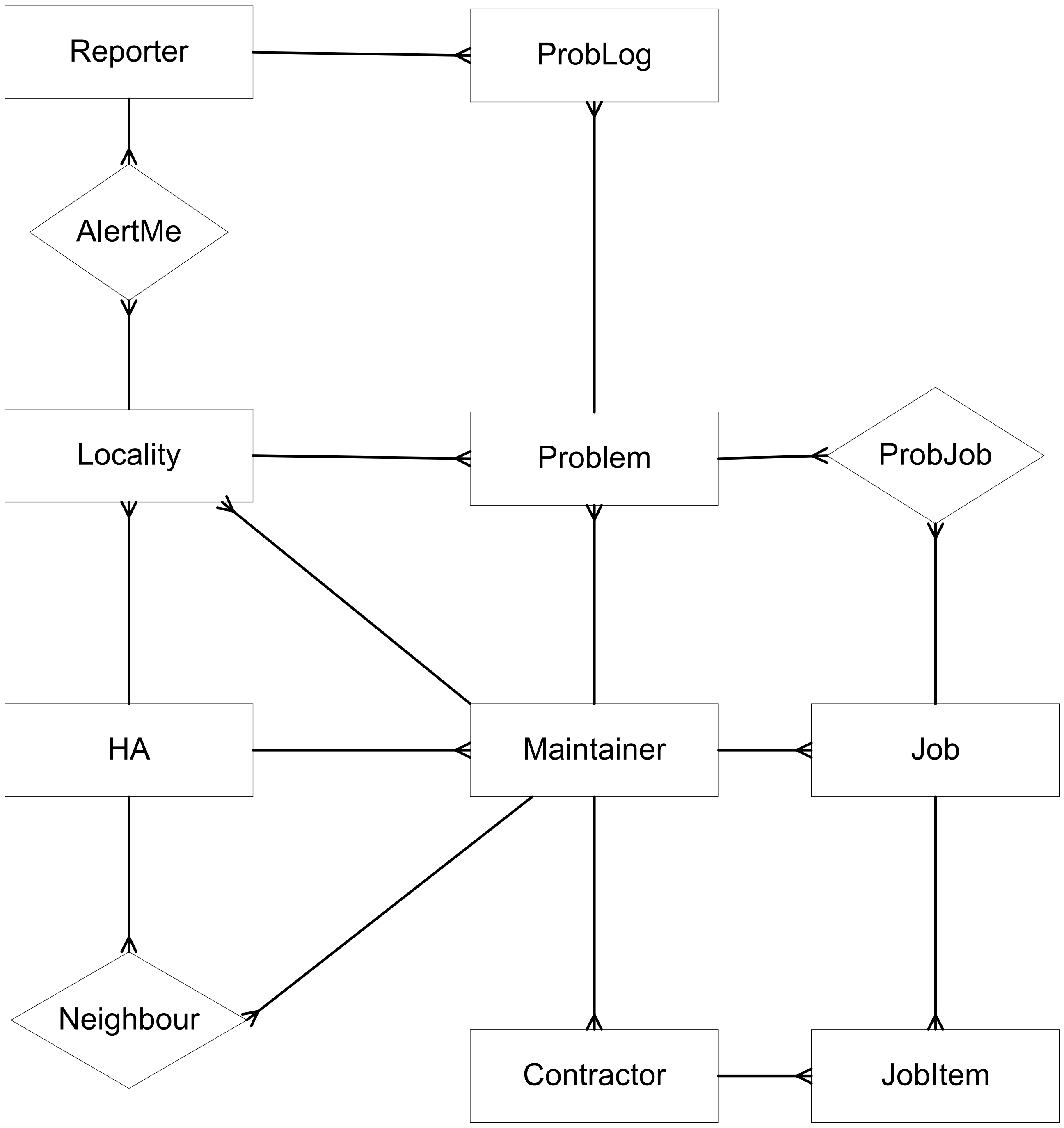
These specifications are illustrative, slightly simplified and subject to adaptation at the detailed design stage.

3.2.1 Table catalogue

Table	Description
AlertMe	Links a reporter to a locality so that they can be alerted when a new problem is posted
Contractor	Contact details for sub-contractors and units. Used for allocating job items to.
HA	Base details of highway authority
Job	Job header
JobItem	Job item
Locality	Places
Maintainer	Base details of maintainer
Neighbour	Links to neighbouring maintainers for the convenience of passing problems across borders.
ProbJob	Links problems to Jobs
Problem	Description of defect
ProbLog	History of correspondence regarding a problem. Connects reporters to problems.
Reporter	Person making a report or asking to be notified about problems in locality
SysLog	System log

3.2.2 Main relations between tables

Table	Relations
AlertMe	Many Reporter. Many Locality
Contractor	A single Maintainer. NB A real world contractor may work for more than one maintainer but this table is for quick reference of the maintainer and may contain information such as cost code or contract number which differs between Maintainers.
HA	Many Maintainer. Many Neighbours Many Locality
Job	Many JobItem
JobItem	1 Job 1 Contractor
Locality	1 HA 1Maintainer Many Problem
Maintainer	1 HA Many Contractor Many Locality Many Job Many Neighbour
Neighbour	Many HA Many Maintainer
ProbJob	Many Problem Many Job
Problem	Many Reprob 1 Locality Many ProbLog 1 HA
ProbLog	1 problem Many Reporter
Reporter	Many AlertMe Many Reprob
ResponseRef	Lookup table to convert one-time command line references to commands. See Appendix A.



Relationships between database tables.

(Link tables shown as diamonds)

3.2.3 Tables defined

The way fields are named is for clarity of description only.

a AlertMe

An entry in this link table means that the reporter wants to be notified of new problems arising in the Locality.

Reporter.ID	Link
Locality.ID	Link
Type	Set of:- New reports/All events/Finished/Complaints We would like to add two additional flags : Future work/I'm a source of local knowledge but at the moment we are keeping the system down to one where HAs and Maintainers *react*. These bring in proactive possibilities which might be a little too advanced for users of a first issue.

b Contractor

Maintainers keep lists of who they get to do the work. This may be individual highway engineers being asked to investigate issues or sub-contractors. Note that if a contractor does work for more than one maintainer then they will have multiple entries in this table as really this is an address book for each maintainer and the details each maintainer uses may be different.

ID	
IDHash	Used for encrypting command line parameters to web pages
Maintainer.ID	Link
Name	Ordinary name
EmailAddress	
EmailAddressOK	Unknown|Bounces|Proved|Stale To start with we have to take an email address on trust. However as soon as the contractor has responded via an active link which we can tell because they will have done a lookup using the ResponseRef table. Mark addresses Stale after say 3 months of non-use. This will probably prompt a double check with the maintainer if the contractor tries to access the system again.
Telephones	
Specialisation	Describes specialist type of work if any
In-House	Y=Works direct for maintainer
Current	N=No longer used (Kept on DB for audit trail)
NewJobFlag	Y=Generally start a new job for each problem N=Normally all work goes on the same job 1=Only ever put one item on one job
CostCodeOrOrderNo	Reference for contractor's paperwork
DefaultPassBack	See JobItem.PassBackReply
Note	Maintainer's own note

c HA

The base information for a highway authority. NB The HA has the responsibility for maintenance but the Maintainer actually does the work. These two logical bodies could be one and the same in practice.

ID	Serial, unique
IDHash	Used for encrypting command line parameters to web pages
Name	Ordinary name
BriefAreaDescription	20-80 words
ProblemEmail	Where problems are notified
ComplaintEmail	Where escalated matters get dealt with
EmailAddressOK	Unknown|Bounces|Proved|Stale
HighwaysHotline	Telephone number
Country	E/S/W/NI
Puff	Blurb about how the HA processes reports
SecurityCode	Human authentication
AccessCode	Login authentication
SysContactName	Contact for System administration
SysContactEmail	
ClientIPMask	Possibly restrict to certain IP addresses
SysNote	Sysadmin's private note
NoOfMaintainers	How many maintainers are currently used? NB if a HA does all its own work then this will be 1 ie. itself.
LastProblemSerial	This counts up sequentially each time a problem report is sent to the HA.

d Job

The header information for a job

ID	Serial,unique
IDHash	Used for encrypting command line parameters to web pages
Maintainer.ID	Link
CostCode	
OwnSerial	Maintainer may have other serial number
Watchdog	Date of earliest outstanding JobItem.AnswerBy

e JobItem

The record of who asked for what to be done and what was the result.

ID	
Job.ID	Link
IDHash	Used for encrypting command line parameters to web pages
DateOfRequest	Date and time
RequestBy	Initials or name
Contractor.ID	Link
RequestText	
AnswerBy	Date by which action/answer is required (Watchdog)
LeaveWithMe	Date by which action/answer is promised
ReplyText	
DoneDate	Date and time

CCOrderRef	Cost code or order reference number
WorkDone	Y=Contractor has done whatever was requested
WorkChecked	Optional text for follow-up by inspector
PassBackReply	Is reply to be passed straight back to ProbLog?

f Locality

Localities are named places as they appear on a map down to hamlet size.

ID	
Name	
Type	Borough|Town|District|Village|Hamlet|Trunk road|Other place
HA.ID	Link (may be missing)
Maintainer.ID	Link (may be missing)
OSMapRefEast	
OSMapRefNorth	
Claimed	0=No 1=By HA 2=By Maintainer. (Initially this data will come from a gazetteer where the information may not be accurate. We rely on HAs and Maintainers to tidy this up either as an exercise or as boundary matters arise.)
Note	Explanation if this causes boundary problems.

g Maintainer

Maintainers are the bodies that organise the actual work. Technically the HA has responsibility but sub-contracted maintainers generally deal with everyday matters. Typically a maintainer will field problems and farm the work out to its own staff or contractors.

ID	
IDHash	Used for encrypting command line parameters to web pages
Name	Ordinary name
HA.ID	Link
BriefAreaDescription	25-200 words
CurrentFlag	Set false when no longer used. (Maintainer's can't be deleted because that would obliterate the audit trail.)
ProblemEmail	Where problems are notified
EmailAddressOK	Unknown|Bounces|Proved|Stale
ClientIPMask	Possibly restrict to certain IP addresses
NewJobMode	Generally speaking, how are tasks assigned to jobs and job items? (These possibilities and rules for combining them with other flags will need further investigation.) For example one possibility is to have one job per problem. Another one job per contract with contractor for which many unrelated job items are added as required. Another is to have each task as a completely separate job: Any Contractor = Look at Contractor.NewJobFlag ProbType = Use cookies to see what we did last time we had this type of problem.

	EachIsNew = 1 job per job item UseExisting = Add job items to existing jobs.
AccessCode	Hash of password allocated by HA.
LastProblemSerial	This counts up sequentially each time a problem report is sent to the Maintainer.
HANote	HA's private note
SysNote	Sysadmin's private note

h Neighbour

This is a convenience link which maintainers and HAs can use to quickly transfer problems across boundaries.

HereMorH	M=Here is a maintainer H=Here is a HA
HereID	Link to HA or Maintainer
ThereMorH	M=There is a maintainer H=There is a HA
ThereID	Link to HA or Maintainer

i ProbJob

This links Problems and Jobs

Problem.ID	Link
Job.ID	Link

j Problem

ID	
Type	Pothole|Bad surface|Blockage|Bad design/construction|Lighting|Signs|Drainage|Vegitation|Other
Title	Brief summary
Narrative	
Locality.ID	Link
Location	Descriptive text
Maintainer.ID	Link
OSMapRef	Text
Status	Reported|Acknowledged|Fixed|Rejected|Chased|Unfinished|Bodged|Re activated
Result	NoFaultFound|Deferred|Fixed|Fixed after chase|Excuse|Dispute|Less than satisfactory repair
NFA	Y=NFA has been posted by maintainer
Watchdog	Earliest outstanding date of expected reply taken from relevant ProbLog.OverdueWatchdog fields

k ProbLog

The events, including the initial report, are listed against a problem. This builds up as correspondence passes and comments are made. It also links reporters to problems.

ID	Unique serial
Problem.ID	Link
Timestamp	
Reporter.ID	Null if generated by HA/Maintainer

<table>
<tr><td>Type</td><td>Report|HoldingReply|Reply|NFA|Comment|Complaint|Satisfaction</td></tr>
<tr><td>Text</td><td></td></tr>
<tr><td>Value</td><td>Multi-use value field.
Report : Risk
Satisfaction : Score</td></tr>
<tr><td>OverdueWatchdog</td><td>Date by which maintainer is expected to reply</td></tr>
</table>

l Reporter

This identifies people who make reports, comments or wish to be notified of problems in their locality.

<table>
<tr><td>ID</td><td></td></tr>
<tr><td>IDHash</td><td>Used for encrypting command line parameters to web pages</td></tr>
<tr><td>Name</td><td>Required</td></tr>
<tr><td>EmailAddress</td><td>Required</td></tr>
<tr><td>EmailAddressOK</td><td>Unknown|Bounces|Proved|Stale
To start with we have to take an email address on trust. However as soon as the reporter has responded via an active link which we can tell because they will have done a lookup using the ResponseRef table. Mark addresses Stale after say a year of non-use. This will probably prompt a double check if the reporter accesses the system again.</td></tr>
<tr><td>Telephone</td><td>May be required for urgent reports</td></tr>
<tr><td>Locality.ID</td><td></td></tr>
<tr><td>PostCode</td><td></td></tr>
<tr><td>Role</td><td>Any relevant role. eg Parish Clerk</td></tr>
<tr><td>ClientIPAddress</td><td>Could be used to short-cut failed ID-by-cookie</td></tr>
<tr><td>AccessCode</td><td>(Hash of) password</td></tr>
<tr><td>SystemBlock</td><td>Code used to deal with abuse and bouncing</td></tr>
<tr><td>LastEmail</td><td>Timestamp. When was the last email sent.</td></tr>
<tr><td>LastAccess</td><td>Timestamp. When was the last site access</td></tr>
<tr><td>LastInteraction</td><td>Timestamp. When was the last ‘submit’</td></tr>
</table>

m ResponseRef

See Appendix A. Implements CA - Cryptic access

<table>
<tr><td>RefNo</td><td>Unique, random 64 bit integer</td></tr>
<tr><td>Command</td><td>String for command line</td></tr>
<tr><td>Expires</td><td>Expiry date</td></tr>
<tr><td>UserType</td><td>Reporter|HA|Maintainer|Contractor
The type of user for whom this command will be applicable. So for example if we know that a user is a maintainer we want to block them from contractor pages.</td></tr>
</table>

n SysLog

Log of recent system activities used to provide diagnostic, security and statistical information to the system administrator. Details will be let until the detailed design and programming stage.

3.3 Database technical issues

3.3.1 Sizing

It is important that the server has enough resources to service requests quickly. The capacity requirement and level of demand can only be estimated, but nevertheless this provides a performance specification which we can use to evaluate server options.

a Assumptions

Area covered: England, Wales and Scotland
Say 50 HAs
Say 10 problem reports per HA per day
Say 30% of reporters being first-time reporters
Say 4 maintainers per HA
Say 20 contractors per Maintainer
Say 25,000 localities
Say each problem results in 20 screen accesses in total
Say 80% of those screen accesses are during the working day of 8 hours
Say each problem results in 5 ProbLog entries
Say each problem results in 8 emails (incl. job items)
Say each problem results in a job and 2 job entries
Say each screen requires 5 database accesses including 2 multi-table SQL queries
Say each email requires 4 database accesses including 3 multi-table SQL queries
Say general public enquiries are not a significant loading
Say each screen is 2K bytes
Say each email is .5K bytes
Say 250 days in a year. (Weekdays is a reasonable measure in this context.)

b General sizing implications of these assumptions

- 500 problems per day - 125K per year
- 150 new reporters per day - 40K per year
- 10000 screens per day
- 17 screens per minute during working day (80% of total)
- 4000 emails per day
- 10 emails per minute during working day (80% of total)

c Database size

We can estimate the number of records and a nominal record size for each table

Table	Record size (k)	Capacity calculation
AlertMe	.05	If 5% of reporters ask to be notified about 2 Localities : 1.5Mb/year - 1550 records/year
Contractor	.25	1Mb
HA	.5	0.1Mb
Job	.05	6.3Mb/Year - 125K records per year
JobItem	.2	50Mb/Year - 250K records per year
Locality	.05	1.25Mb
Maintainer	.3	0.1Mb
Neighbour	.03	If each maintainer and HA has 4 neighbours: 0.1Mb
ProbJob	.03	Essentially a 1:1 relationship. 4Mb/Year
Problem	.3	38Mb/year - 125K records/year
ProbLog	.06	37Mb/year - 625K records/year
Reporter	.15	6Mb/year - 40K records/year
ResponsRef		20Mb - 450K records (pessimistic)
SysLog		This will be weeded/archived frequently. A week's logging might be 10Mb but this would then be cleared.

The simple (and simplistic) totals are

Static size	3Mb
Yearly growth	125-150Mb

If we assume that we keep

Jobs/JobItiems for 1 year
Problems/ProbLogs for 5 years
Reporters/AlertMes for 5 years

then the capacity required will eventually become

Static tables	23Mb	
AlertMes	7.5Mb	8K records
Jobs	7Mb	125K records
JobItems	50Mb	250K records
ProbJob	4Mb	125K records

Problems	190Mb	625K records
ProbLog	185Mb	3.1M records
Reporter	30Mb	200K records
giving a total of	500Mb	

(Which is 760bytes per problem/5 years or a back of the envelope value of 4K bytes per problem per year for the amount of database storage required.)

d Performance

One of the important parameters of the database specification is the number, complexity and bytes to be returned at peak periods. Let us assume that peak loading will be twice the average load through the day with 80% of activity occurring in the 8 hours of the working day.

	24 hours	Per minute (peak)	Seconds allowed
Screens	10000	33	
Emails	4000	13	
DB accesses		220	.27
Multi-table SQL		107	.56

e Discussion

The large number of records in ProbLog might be cause for concern. It may be that efficient indexes will mean this is a non-problem, or it might be better to archive after say a year into a text log file format which becomes part of the problem record.

In any event, indexing of hundreds of thousands of records will be critical to performance.

It is difficult to make an accurate assessment of the amount of database work required over a variety of screens. Therefore we have selected what we think are reasonable values for this level of design.

3.3.2 Monitoring

There are three sorts of monitoring we need to carry out

a Ensuring the system is up and live

A test query every couple of minutes with a maximum delay time-out will be used to verify the system is capable of responding to queries. This might be a stand-along cron job or incorporated into a check that page serving and the database are working.

b Measuring response times and usage

The data required to prove levels of service and if necessary alter the level of resources needs to be collected and averaged for statistical purposes.

c Periodic checks on usage

To enable policy decisions to be reviewed in the light of more definite data.

3.3.3 Backup

Losing a day's transactions is not acceptable, there might be urgent requests to look at dangerous defects which get lost. Therefore the database at least needs to be mirrored either in real-time or very frequently.

3.4 Confidentiality and security issues

3.4.1 Personal data

We collect very limited personal data about reporters. This is required to allow Maintainers to make further enquiries and desirable so that they can respond. But we don't ever publish the reporter's email address, not even to the maintainers. We don't collect the full postal address but in the event that it is imperative to find the person we hope to have enough information to allow a determined searcher to find them. An instance of this would be where an accident investigator wished to take evidence from a reporter.

We can't see any reason to provide anonymity.

3.4.2 Commercial data

One of the reasons for the split between problems and jobs is to allow the latter to be kept between the maintainer and the contractor.

It is proposed to allow access for auditing, but the tools and access controls for this have not been considered in detail. Probably each HA will be able to appoint an auditor with access to the sorts of information described in section 2.5.5.b.

3.4.3 Access controls

a Reporters

We expect most reporters to use the same computer for their reports and so the use of cookies to identify them quickly and without the user needing to remember a password is viable. In effect the system can say "we recognise you as we've seen you before".

When we send emails to Reporters we pass them their IDHash to use as an identifier rather than a plain serial. The system identifies people by their email address and will offer to save a password and send it to that email address if requested.

b HAs

The system will deal exclusively with HAs who will then be responsible for allocating passwords to their maintainers.

Because of aspect of 'we the Maintainer commission you the Contractor to do some work for us' we insist on authenticated logins from Maintainers (and HAs). Contractors don't really need authenticated logins or passwords because they are always replying to emails which will have been sent from Maintainers which use a difficult to guess ID hash rather than a plain serial.

When we send emails to HAs and maintainers we pass them their IDHash to use as an identifier rather than a plain serial.

3.4.4 Dealing with abuse

At this stage it is difficult to tell exactly what abuse will be significant. We will probably have to wait for feedback from annoyed parties before being able to deal with it effectively and without interfering with legitimate activities. (For example it may be perfectly legitimate for somebody to report a dozen defects in one go.)

Reporters giving email addresses that bounce will be blocked.

Note that no email addresses of reporters, HAs, Maintainer's or Contractors are ever published or made known to 3rd parties.

3.4.5 Dealing with dozy users

The normal way to respond to an email is to click on the 'reply' button. However we don't want this to happen because we are forcing people to use web pages to ensure that the database is kept in the loop.

We suspect that the biggest difficulty will be with HAs and Maintainers who have to follow a protocol. This isn't difficult, and the options will be laid out in the email in active links with explanations built-in, but even so we expect people will get into a mess.

As the system administrator has the email addresses of all participants it would be possible to send reminders and clarifications when problems like this occur. Therefore we will provide such a facility for the system administrator.

4 Screens and emails

In section 2 we discussed what functions the system would perform. Now we describe the practical matters of the user interface to implement these functions in a way that appears logical and consistent to the users.

4.1 Scope of design

4.1.3 Logical screen structure

In the following we explain the *logical* structure and content. Details of design, particularly the *appearance* will depend on the way programmers chose to implement the system. Screens shown here as separate may be merged. For example "Search and select a locality" might be a separate screen with an excursion or built-into a screen where we need a locality - Of course what actually goes on beneath the surface should not affect the way users experience the system.

4.1.2 User interface

In the detailed development we expect the following matters to be given more attention:

- We assume that most users are unfamiliar with the system. Therefore we will want screens and emails to be carefully constructed and tried-out on novices.

4.1.3 Database operations

We have not gone into much detail about the database activities associated with screens and emails because we feel that the context makes it clear what is to be retrieved and updated.

4.1.4 Security

This is discussed further in 4.8. In simple terms we expect HAs and Maintainers to have secure logins, Contractors to rely on CA via email and Reporters to use a combination of CA, cookies and self-selected passwords.

4.2 Common characteristics

4.2.1 Basic paradigm

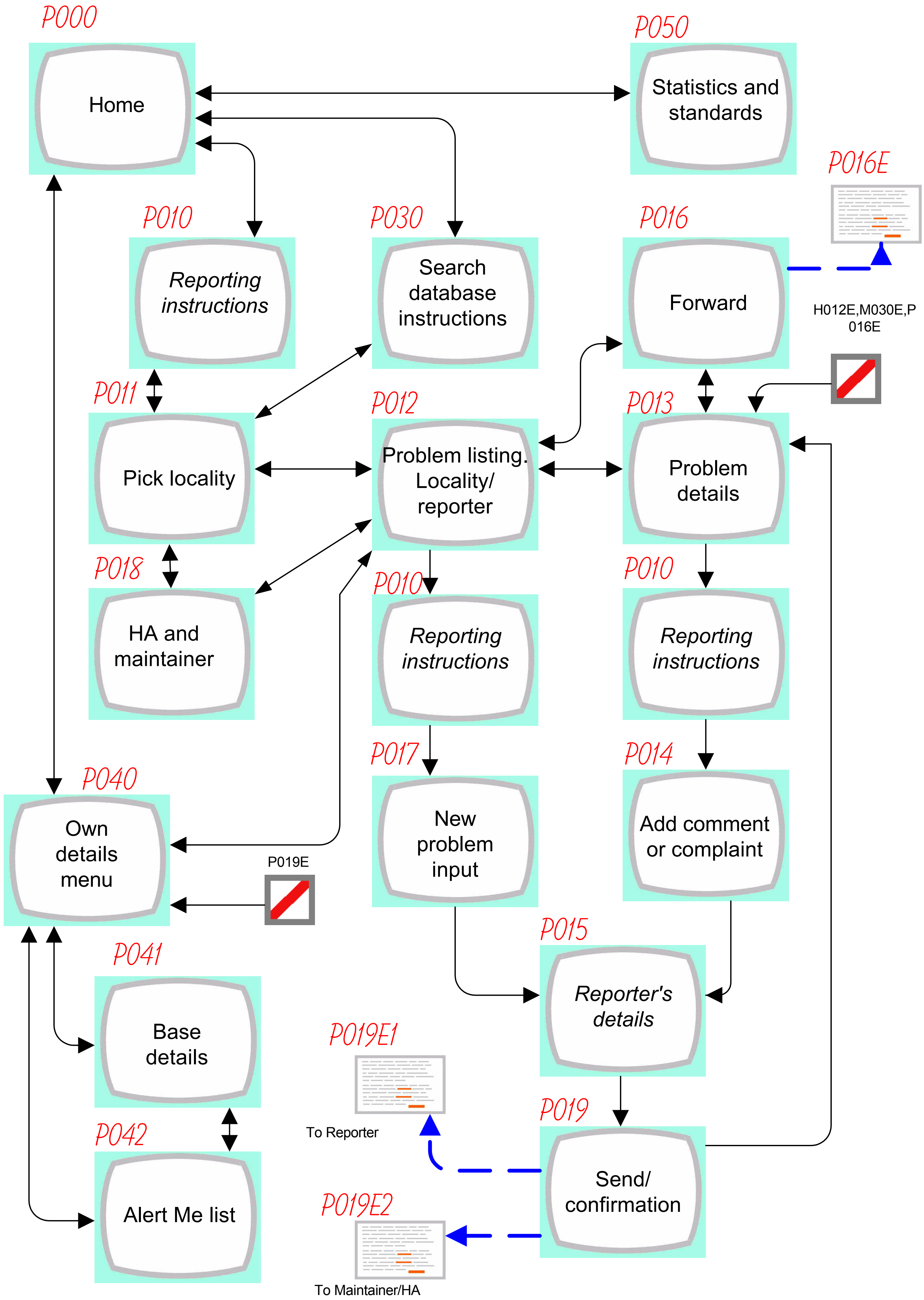
Everything happens on web pages with results appearing as system-generated emails. These emails contain enough information and options in active links for the recipient to get to exactly the right web page with a single click.

4.2.2 CA

We will be using Cryptic Accessing as described in Appendix A. This means that we can do some simple assurance of who is trying to access a page. This is not a substitute for proper user authentication where that is used, but may be a powerful short cut elsewhere.

4.2.3 Welsh

We may have to adapt these screens to work in Welsh. This complication needs to be thought through when implementing screens. It is conceivable that we might have to write one email in Welsh and a copy in English. At present we raise the issue without taking steps to implement it.



Public and reporter's screens

Idempotent screens shown in italics

4.3 Public pages

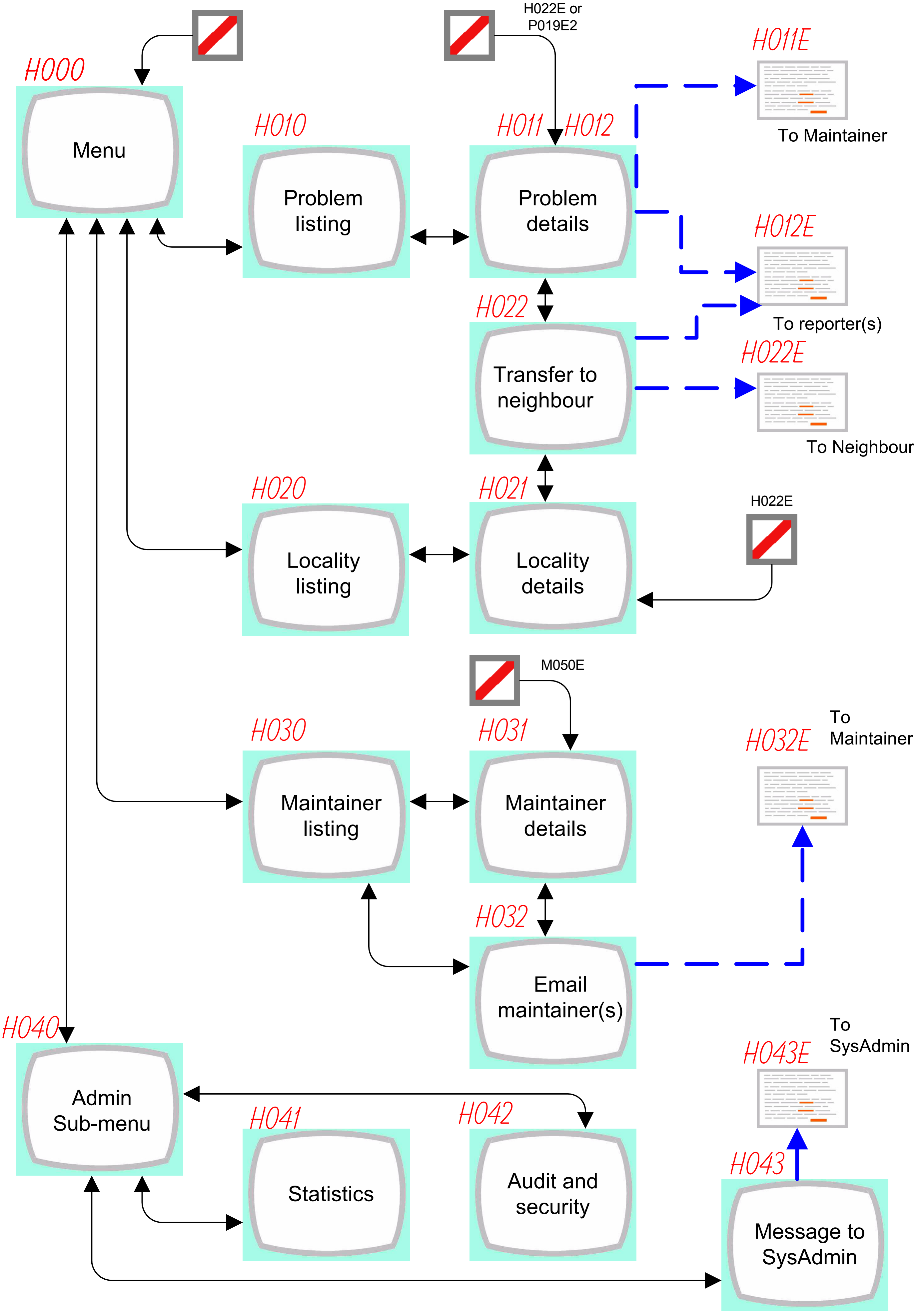
The general browsing public will have access to a bit about the NatPot system, the ability to search the database and to be able to view statistics. To be able to interact with the system and provide reports or comments we need the person's basic details to be able to respond to them. We also need to give them instructions and explain how the system works. Giving instructions and getting details must be done once each session but otherwise we don't need to repeat them.

P000 Home page	This will describe the purpose of the site and give an overview of how it works. Display a warning about reporting critical matters the police. The main links will be > Report a problem with road maintenance > Search the database of defects > Own details (If we know who the user is by cookie) or > Register details (if we don't know the user) > Statistics and standards If we know (by cookie) that the user is a HA or maintainer, provide a link to the appropriate menu H000/M000. If we know the user is a contractor (by cookie) then explain they need to use an active link from one of their emails. (The difference between HAs and Maintainers on the one hand and Contractors on the other is that Contractors don't have authorised logins and therefore we make sure they have received an email from somebody who does using the CA system.)
P010 Reporting instructions (Idempotent)	There are a number of things that we have to explain to reporters: • What sort of things are appropriate • Checking up on existing reports first • The steps to make a new report of follow-up • What happens next • Privacy and own details We need to implement some logic such that this always gets shown once (but only once) per session if the user is reporting or following-up. The way we present these instructions will need very careful design and integration with the other screens so that they are plain, comprehensive and intrude enough to stand out while not being too much bother to read. We may find that separate screens is not the best way to do this.

P011 Pick Locality	The function of this screen is replicated elsewhere through the system although implicitly rather than as here explicitly. In this instance we propose to use cookies to store a recently used list together with a list obtained by recent problems with which the reporter has been involved. To this list we add names found by matching inputted text eg a bunch of 'Stourton's with their county/HA/maintainers listed with them. This list can then be picked from.
P012 Problem listing	This adaptable screen can be to display problems for a locality or a reporter. Provide selection, sorting and format options. Provide clear links to calling screens and P000. Provide a link to HA and maintainer details. (Or incorporate on screen) Each problem can followed to show details.
P013 Problem details	This will show the full *public* record for this problem ie. Problem and Problem Log. Follow-ups (P014) start from here. This page will be referred to by active links in M030E and H012E. Provide a link (P016) to forward the text or link to a third party. Technical note: We may have arrived here by an active link. So we need to know how to get to the 'parent' P012 with the right locality.
P014 Add comment or complaint	(Via P010 if necessary.) This is a simple text message input screen. The nature of the message can be simply categorised, but without any of the detail required for the original report.
P015 Reporter's details (Idempotent)	At this point the reporter has inputted some data but it has not yet been accepted. We must make it clear that the report is not yet complete. The minimum requirement is an email address, but we also ought to insist on a name. For the first time ever we should establish if the user can be identified by cookie or if we are going to give them/ask them for a password/access code. We can present the privacy implications immediately in this case. For the first time this is called in a session we want to check the details are still correct. For following calls in the same session we can skip this or allow it to be called on request.

P016 Forward problem to 3rd party	We allow any member of the public to forward either the URL or the text of P013 to a 3rd party. Important note: This email will come direct from the user's email not via the NatPot system.
P016E Forward problem to 3rd party	When listing the details put an active link to P013. We should to try to ensure that it isn't represented as being generated by the NatPot system but is a private email.
P017 New problem input	Once we have a locality there are basically three more things we need to collect: 1 Location - A more specific spot where the problem lies. This is a very tricky issue because reporters don't go out with plans and theodolites, their references may be vague "just past the farm" or quite specific but difficult to interpret by highways people "right outside the old telephone exchange", or the place may be difficult to describe anyway "On the lane with no name halfway between X and Y". This where getting it right first time is very important and will save a great deal of fruitless searching and correspondence. 2 Problem description - The type of problem can be categorised but then we need to allow the reporter to add a note if they wish. For example 'Pothole' and "Heavy rutting is breaking up the surface for 10 yards". We ask for a title in the same way as a subject in an email so that the thread is obvious. eg "Pothole at Snows corner" 3 Seriousness - The reporter may be reporting a 'stitch-in-time-saves-nine' or a cause of an accident, or something in between. This helps prioritise the work when it arrives at the Maintainer. From here go to Reporter's details (P015) but see that screen for possibilities of skipping. Note though that if a problem is reported a serious then we insist on being given a telephone number to get back to the reporter, so our logic must trap this case.
P018 HA and Maintainer	This screen lists the details of the HA and maintainer for a locality. People might use this if they want to access them outside the NatPot system but want the contact details. This screen is accessed via pick locality (P011) or problem listing when in Locality mode (P012).
P019 Send/ Confirmation	We need something to (a) confirm all the details are correct (b) tell the reporter that the problem has been accepted and when to expect a reply. When finished go to (P013) the problem details.

P019E1 Initial feedback to reporter	We send an email back to the reporter to confirm that the problem has been recorded, repeat the what happens next and provide active links to P013 and P041 NB we need to trap bounces and block the account.
P019E2 Problem notification	This will normally go to the maintainer unless the locality has not been assigned or the maintainer has been marked no-longer active by the HA. As well as the problem details we put an active link to M021 or H011. Add a serial number which counts up sequentially for problem reports to this Maintainer/HA. This gives them the opportunity to make their own records or trap losses. NB we need to trap bounces.
P030 Search database	Introduce the way the database is structured by Locality and what sort of information in contained in it and what the limitations are. Lead onto P011.
P040 Own details menu	We might arrive here as an unknown person from the main menu or as a known person from anywhere or via the active link in P019E1. This could be incorporated into P000 but there may be authentication benefits in keeping them separate. Known users may not need the full blurb but give them an option for getting it. The link to P041 will be marked Create or Edit. we will need to provide some 'I have forgotten my password' method.
P041 Reporter's details	Straightforward edit/input screen. We don't allow reporters to be 100% deleted because that could upset the audit trail. However we will allow them to be deactivated so that when all reports relating to them have been archived they can be removed.
P042 Alert Me list	An optional list of localities which reporters can use to request notifications by email. Provide tuckboxes to switch on/off the options in AlertMe.Type and a remove tick.


H000
Menu
H010
Problem listing
H011
H012
H022E or P019E2
Problem details
H011E
To Maintainer
H012E
To reporter(s)
H022
Transfer to neighbour
H022E
To Neighbour
H020
Locality listing
H021
Locality details
H022E
M050E
H030
Maintainer listing
H031
Maintainer details
H032E
To Maintainer
H032
Email maintainer(s)
H040
Admin Sub-menu
H041
Statistics
H042
Audit and security
H043E
To SysAdmin
H043
Message to SysAdmin

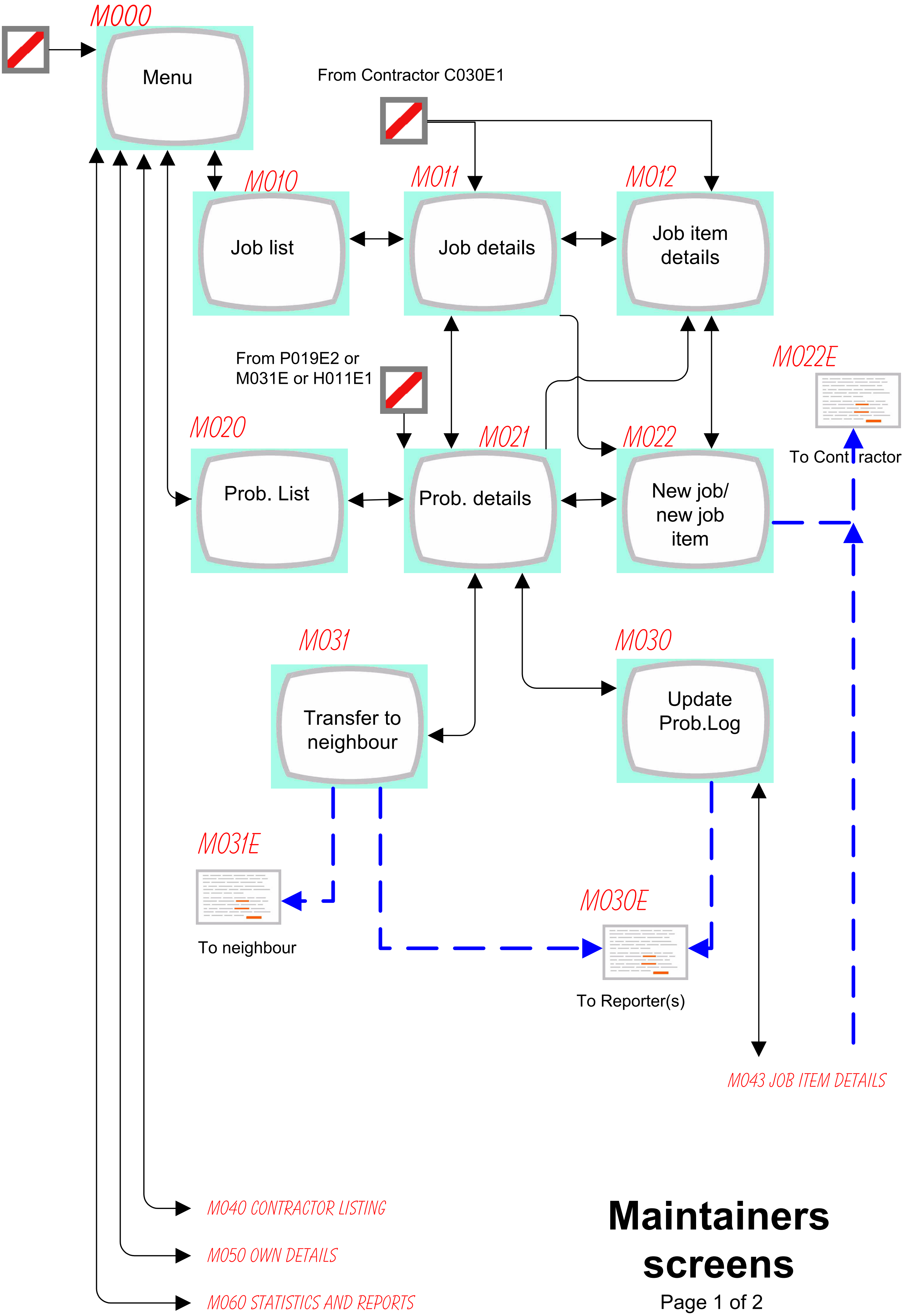
HA's screens

4.4 HA pages

H000 Menu	Accessing this screen for the very first time relies on receipt of an email with a Cryptic Access. This can then be bookmarked. As well as being difficult to find at random it also requires authentication by password. Authentications will be logged. Possibly lock-out multiple instances of the same user. There may be a MOTD. > Problems > Maintainers > Localities > Administration
H010 Problem Listing	There are many possible variants based on searching, selecting, sorting and screen or printer-friendly formats. Store the settings using cookies. The screen versions will have various follow-up buttons: Details, Pass to maintainer, Pass to neighbour, Add item to problem log, Pass to complaints/not maintenance.
H011 Problem details	Quite an important screen. A lot of information to be displayed with various options to follow. Active link to here from initial notification and follow-up correspondence from reporters and maintainers. Display • Basic problem information • Problem Log • Related Job items. The Job Item information will be much sketchier than the Maintainer's version of this screen M021 but will give an overview of what happened when. >Pass to maintainer >Update problem log (and so reply to reporter)
H011E Notify Maintainer	Pass this problem to a maintainer. Active link will point to M021.
H012 Update problem log	[Shown combined with H011 on diagram] See M030
H012E Notify Reporter(s)	See M030E

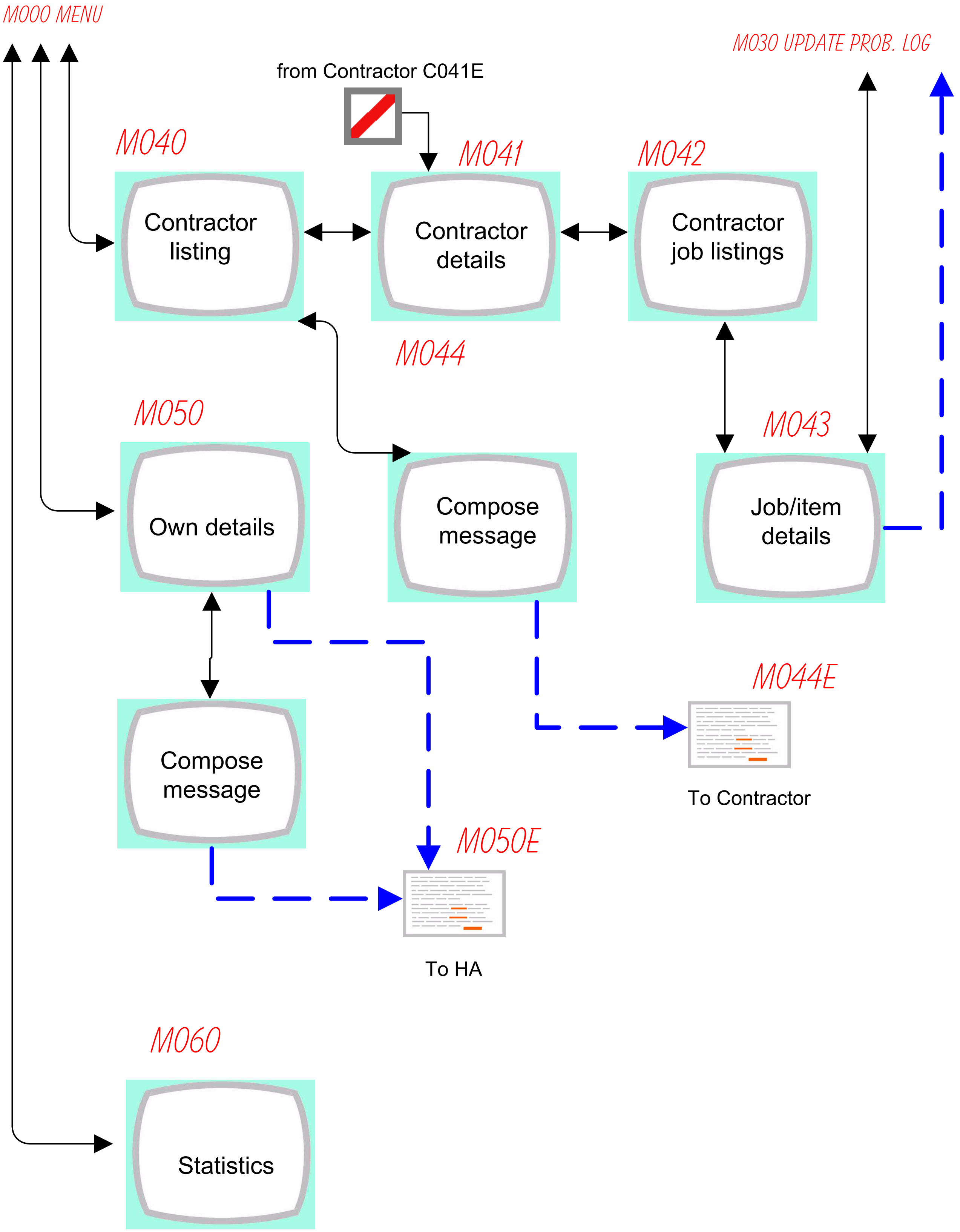
H022 Transfer to Neighbour	The neighbour in this case would be a peer ie another HA. In effect this is a matter of selecting from a list of neighbouring HAs and remembering neighbours for future quick access. As well as sending a notification to the Neighbour, the ProbLog is updated causing notifications to go to Reporter(s).
H022E Notify Neighbour	When we tell a Neighbour that we have dumped a problem in their lap we may also want the definition of the locality reviewed to clarify boundary matters for the future so the active links are to H011 and H021.
H020 List localities	The HA has complete control of localities in two respects. 1 In HAs area? 2 Which maintainer covers it? We anticipate about 500 localities per HA and perhaps half a dozen maintainers. Initially localities will be obtained from OS gazetteer data but these will need to be pruned and adapted as experience shows inaccuracies and confusion. This table could be shown in a variety of formats with selection, sorting and printer-friendly versions with settings saved using cookies. One format might contain a grid of tick-boxes with one column for each Maintainer, one for not this area and another to implement a deletion. There will be opportunities to add and modify localities.
H021 Locality details	Locality maintenance screen. It may be found useful to add local notes such as 'Includes river Avon crossings' in the notes. If the HA wants to pass this onto a Neighbour then link to H022.
H030 Maintainer Listing	List of current (and optionally previous) maintainers. We anticipate that a HA would have about half a dozen Maintainers. The list will have tick boxes to send the same email to all those ticked via H032.

H031 Maintainer details	The HA has complete control over the Maintainer's details. If changes are made send H032E which points to M000 (NB Not M050 - There will be a very first time and that's when we need the maintainer to start from their menu with the appropriate security procedures.) Conversely we may have been sent here as a result of the Maintainer changing some of their own details. This means the HA can vet the changes. Part of setting up a new maintainer and good security practice is for the HA to allocate a password to the Maintainer (which is needed to access their menu.)
H032 Email Maintainer(s)	Simple input and accept screen for email text.
H032E To Maintainer	Active link points to M000
H040 Admin sub-menu	There may be additional security restrictions here. > Reports > Auditing and security > Contact NatPot sysadmin
H041 Statistics and reports	Various summaries in printer-friendly format. Typically these will be general performance figures.
H042 Audit and security	What happens here needs to be investigated further. We anticipate some access to the Job and Job-item records of maintainers on a comparative basis to try to extract costings and where delays occurred.
H043 Create email for sysadmin	Simple input form resulting in H043 being sent to NatPot system administration.
H043E To sysadmin	



Maintainers screens

Page 1 of 2



Maintainers screens

Page 2 of 2

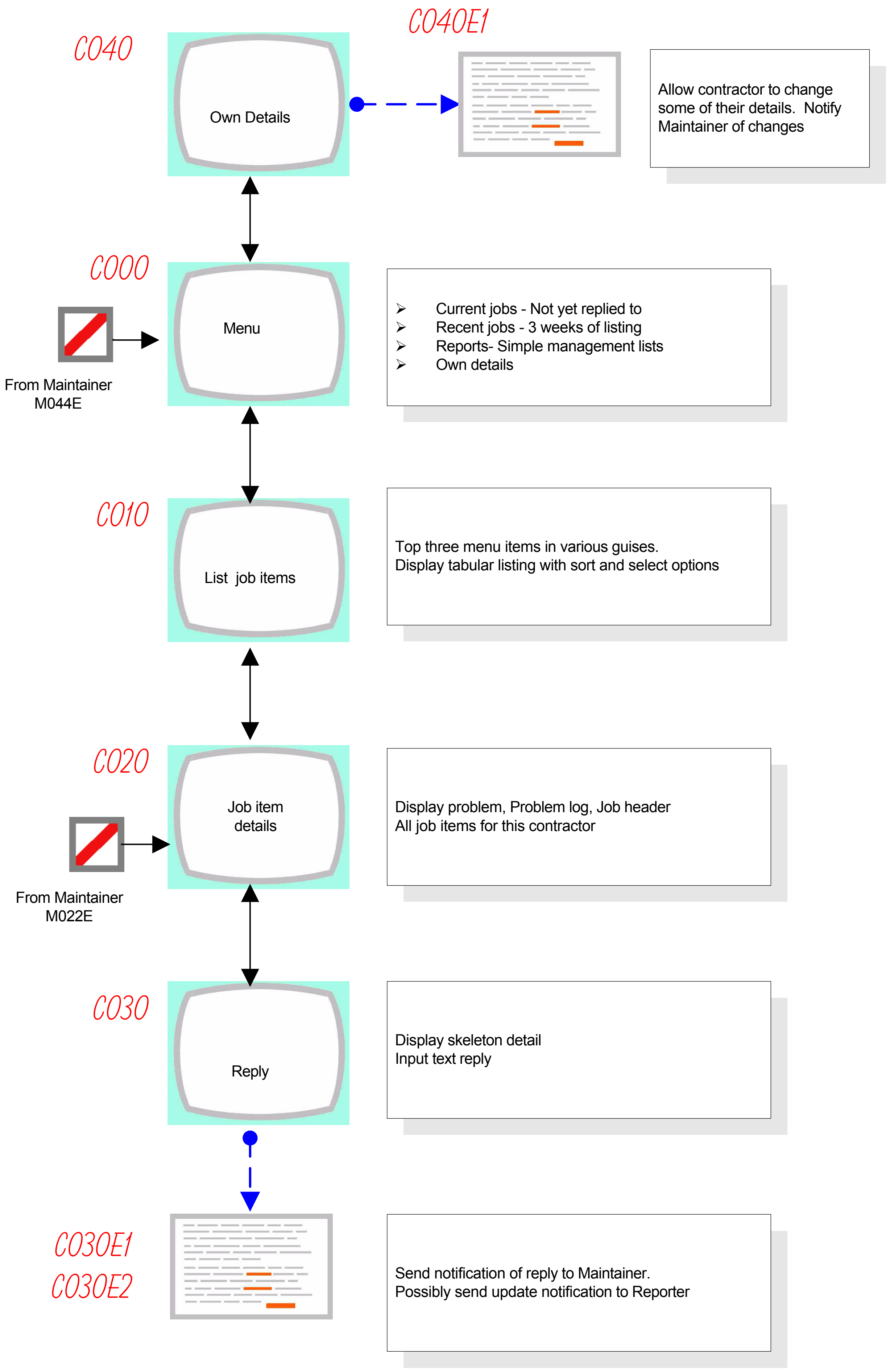
4.5 Maintainer pages

M000 Menu	> Job listing (various options) > Problem listing (various options) > Contractor listing > Own details > Statistics and reports This is bookmarkable There may be a MOTD
M010 Job listing	We will provide a variety of job listings, but all will be variations on the same theme. Provide facilities to sort, select and adapt presentation for screen/printer. Some will undoubtedly relate to (outstanding) job items so as well as selecting we may provide a display of job items as well. Remember preferences in cookie. Locality.name Locality.ID=Problem.Locality.ID Problem.Type Problem.Title Problem.ID=ProbJob.ProbID ProbJob.JobID ProbJob.JobID=Job.ID Job.Watchdog Job.*various* JobItem.various JobItem.JobID=Job.ID . . . where Job.MaintainerID=*Maintainer*
M011 Job details	The details to be displayed are: Basic problem information, Job header and all job items. Active link from C030E which is a contractor's reply to a job item request.
M012 Job item details	Display the background information (Basic problem information and job header) Display the job item. Links (or ready-on-screen) to update problem log (M030) and create a new job/job-item(M022) Allow the status to be updated
M020 Problem list	Variations on a theme. Sort, search and select. Different formats for screen/printer. Remember preferences in cookie.

M021 Problem details	Quite an important screen for a maintainer. A lot of information to be displayed with various options to follow. Active link to here from initial notification and follow-up correspondence from reporters. Display • Basic problem information • Problem Log • Related Jobs and Job items. >Create new job/job item >Job details >Job item details >Update problem log (and so reply to reporter)
M022 New job / Job item	The exact use of jobs and job items will probably vary. Some jobs will be call-off contracts with many different job items going on it over a period. Others will be jobs specifically set up for the purpose. We can envisage a particular contractor with a single job in which case we can help the maintainer by allowing them to select the Contractor first then have the last Job 'number' displayed for "use this job or start a new one". Contractor.NewJobFlag and Maintainer.NewJobMode.
M022E Notify Contractor of job item	Using the contact details in the Contractor record send an email with problem description and any problem log entries, Job header and job item details. Make clear which maintainer it is from. Put in an active link to C020 (and possibly C000). We may want to log this as part of an audit trail with details of the user and machine identity. Clearly there must be heuristics we might use to spot unusual patterns of allocating jobs.
M030 Update problem log	Feeding information back to reporters is one of the key activities for maintainers, This screen (as well as the display of the problem, log so far and job items) will be mainly a text input with buttons for codifying the type of response.
M030E Notify reporters of update	Using the input from M030 this gets sent to all reporters and anyone who has asked to be kept informed. Put the problem title in the subject line, keep the message brief, include an active links to P013 problem details page. Note that although each recipient will be pointed to P013 because we will include their reporter.ID in the command line each will have a different reference number in the active link.

M031 Transfer to neighbour	There will be many cases where a report is sent in good faith to a maintainer but lie 'across the border' in another's patch. Therefore we need a way to pass it on. This screen provides a picklist of known neighbours (known because we have been here before and remembered them) and a search/select from all maintainers. (This may have to be two screens). If we select another maintainer then trigger two emails (reporter M0301E and new maintainer M031E1). If we are flummoxed then pass by email to HA M031E2.
M031E1 Transfer to maintainer	This is a duplicate of the initial problem report with the addition of a not-our-patch reason for transferring.
M031E2 Unknown location	Forward the initial report to the HA with a 'not-our-patch' and 'but-can't-find whose patch' addition.
M040 Contractor list	A maintainer will have a roster of staff and sub-contractors. This table will be supplemented by an add button. The table will show all the contractors for this maintainer, possibly in different formats and with sort options. In order to allow emails to be sent to a bunch of contractors the list will be provided with tick boxes and an 'email these ticked contractors' button leading to M044.
M041 Contractor details	The maintainer has ultimate control over contractor details. This screen will be accessed directly by active link in C041E (Contractor changes their details) For convenience this might include outstanding job items.
M042 Job/Job item listing for contractor	Various selection and sorting options. Opportunity to search text. Varying tabular formats for screen and printer. Each row will lead to details M043
M043 Job item details	The job item details will typically be used to examine the response from the contractor. This can then lead to updating the problem log M030. Also provide the facility to send a follow up to the Contractor using M022E
M044 Compose message to contractor(s)	This might be incorporated into M040, but as we anticipate it won't be used very often it might be best to keep M040 uncluttered. A simple input for message text and send button.

M044E General email to contractor(s)	As well as text payload, put an active link to C000. Logging as per M022E
M050 Own details	Straightforward maintenance screen. There must be some access controls and logging. Not all fields are self-alterable. After alterations are made send M050E to HA.
M050E Change notification	The purpose of this is to alert the HA to changes made to the Maintainer's details by the maintainer. Include an active link to H031
M051 Message to HA	General purpose text input for email to HA. Might be incorporated into M050. Create M050E or slight variant.
M060 Statistics	Summary statistics. Possibly leads to more detailed statistics in printer-friendly format.



Allow contractor to change some of their details. Notify Maintainer of changes

- Current jobs - Not yet replied to
- Recent jobs - 3 weeks of listing
- Reports- Simple management lists
- Own details

Top three menu items in various guises.
Display tabular listing with sort and select options

Display problem, Problem log, Job header
All job items for this contractor

Display skeleton detail
Input text reply

Send notification of reply to Maintainer.
Possibly send update notification to Reporter

Contractor's screens

4.6 Contractors pages

C000 Contractors menu	We may want to refer Contractors to this general purpose screen by active link. It wants to be bookmarkable using contractor.IdHash. All the menu options except Own Details are variations on a theme - pointing to C010
C010 Job item listing	This is a table in varying formats (one being printer friendly) with various search, selection and sorting criteria. In some versions there will be links to C020. Remember preferences in cookie. Skeleton for SQL:- Locality.name Locality.ID=Problem.Locality.ID Problem.Type Problem.Title Problem.ID=ProbJob.ProbID ProbJob.JobID ProbJob.JobID=Job.ID Job.MaintainerID Maintainer.Name Maintainer.ID=Job.MaintainerID Job.CostCode Job.ID=JobItem.JobID Job.OwnSerial JobItem.*Various* . . . where JobItem.ContractorID=*This contractor*
C020 Job Item details	Display background information about the problem and job but only the job items relating to this contractor. Problem(1), Problem Log records(1-many),Job heading(1),This job item, Any other job items for this contractor (0-many).
C030 Reply to job item	[This might be incorporated into C020] Input for text reply. Tick for 'completed' (as opposed to holding reply). Submit updates the Job Item record, sends C030E and possibly sends C030E2 depending on JobItem.PassBackReply flag.
C030E1	Email to maintainer embodying reply. Tell if reply has been passed to ProbLog Active link to M011 and M012
C030E2	Email to reporter(s) if JobItem.PassBackReply flag is set true. See M030
C040 Own details	Only allow access here if we have come via the

4.7 System administration

4.7.1 System administration overview

There are two types of system administration:

- Administering hardware, communications and databases
- Administering operations within the database and with users

The first is dealt with in section 5. Here we consider only those activities which might be called housekeeping and surveillance related to the system that runs 'on top of the database'.

We anticipate that the majority of administration will be routine surveillance with regular running of utility programs. Occasionally a more knowledgeable and in-depth response to a situation may be required.

4.7.2 Setting up for first time

a Gazetteer

We may be setting this up using data supplied by the Ordnance survey. This will need checking and possibly adaptation. Given the number of Localities involved (we are looking to have about 25,000 but the original data set may be an order of magnitude larger) most of this will have to be done mechanically which is beyond the scope of ordinary administration. However there may need to be some further tweaking, such as for example adding in Trunk roads which as far as we are concerned are distinct from their surroundings (because they are looked after by the Highways Agency) and may not appear as such in the original dataset. Therefore we need a Locality maintenance facility.

b HAs

We need to populate the HA table with bare bones information before we can 'rope them in'. Also HAs will be using authorised access so that means we need to be able to set and reset passwords. Therefore we need a HA maintenance facility.

We expect the broadcasting of messages to HAs (see 4.7.6.c) to be a frequent occurrence in this period.

c Trial period monitoring

We envisage a nation-wide trial period. During this period we expect HAs, Maintainers and Contractors to familiarise themselves with the system using test data. The administrator will have a statistical monitoring program to see how much activity is happening in each HAs area and a utility for generating test reports.

4.7.3 Routine operations

a Dealing with correspondence

HAs have the facility to email the system administrator. (Maintainers will have to go via their HAs.) We anticipate the usual spread of support queries some of which are routine and others require careful handling for security reasons or more in-depth management response.

When sending email in reply there needs to be some authentication, perhaps a digital signature or a checkable CA link which is difficult to forge.

b Generating periodic reports

The statistical reports for public display, and performance monitoring will be produced periodically and then filed for 'the record'. The technical side of this is in the programming while the operational side will be simple procedures.

4.7.4 Monitoring and management

a Usage statistics

Some facility to view the workload load and size of the database in quantative terms. (This will be complimentary to database performance statistics.)

b Filing bug reports/change requests

HAs have the facility to email the Sysadmin. We expect other feedback to arrive via the Syaadmin. Yet they are not in a position to change anything, although finding out what the real problem is in terms that system technicians can understand is important. When there is something definite being suggested this can be passed to technical support.

4.7.5 Exception monitoring

a Log files and spotting unusual behaviour

The daily processing of logs such as daily filing can be done automatically. Most log entries will never be used but occasionally they may be used for following an audit trail or more urgent occurrences. For example a Maintainer who enters reports may be creating false work for themselves or crony contractors.

Due to the varied (and evolving) nature of strange goings-on we start by getting a human system administrator to examine the log entries. Therefore we need to provide the system administrator with a flexible log file extraction tool.

b Bouncing email

When email is bounced the follow up action depends on where it has bounced from.

HA	Syadmin to chase.
Maintainer	Automatically notify HA (and possibly sender)
Contractor	Automatically notify Maintainer
Reporter	Automatically mark the Reporter record as bouncing and stop sending email

The first of these requires the sysadmin to take action. However as well as that we want to be able to *suspend* emails to HAs and Maintainers as their bounce problems are likely to be due to mail system failures rather than 'gone-away'. The implication is that as soon as we get a bounce from one of these addresses we have to store or be able to recreate emails in order to resume service later and clear the backlog of mail to them.

Therefore we need to provide controls and overview of outgoing emails. This might be connected with the log file system.

4.7.6 Occasional operations

a Weeding

From time to time obsolete records will be purged. From the Sysadmin's point of view this is a procedural matter.

b 'Hacking' data that can't usually be altered

For example HAs cannot change their name at will. Therefore we need to give the Sysadmin the ability to make alterations to otherwise immutable data. We would expect this to be done under the supervision of technical support.

c Sending messages to users

- There will be a simple MOTD function which allows all users to see a message on their web pages. For example "System will be shut down on Thursday 1am - 5am".
- There will be a similar facility to configure the signature text on emails.
- From time to time the Sysadmin will want to send circular messages to HAs regarding general points about how the system is being operated and reminding them of good practice.
- The Sysadmin needs the facility to be able to email anybody on the system.

4.8 Access control

There are five types of user to which we can apply different security policies.

General public	Unrestricted access to public pages
Reporter	Identity tied to email address. Supported by cookies. If cookies don't work then access requires a password. A screen function/email is required to deal with forgotten passwords. Reporter can access their data, Alert-Me and make reports, comments and complaints. The system may automatically revoke access permissions or the Sysadmin may do likewise.
HA	An HA is the source of access permissions for Maintainers (and they in turn control the access of Contractors). The System administrator controls the access of HAs. All HA access must be by authorised login. (ie type in user name and password) before being allowed to proceed. The Sysadmin may revoke access permission.

Maintainer	Maintainers must use passwords under the authority of the HAs. All access will be via authorised logins. The HA and Sysadmin may block access. Maintainers are forbidden to act as Reporters because of the risk of fraud and massaging statistics. We can trap most of this through monitoring IP addresses but will not be able to eliminate outside cronies. (But the public nature of the system should be a bit of a deterrent.) But see section 6.5.1 below.
Contractor	Contractors have limited access because the CA system points them to specific job items. The emails containing these job items must have originated from a Maintainer (which must have access authorisation.) Therefore, providing we identify the contractor and the job item in the CA we can give them access to job and their own records without having to manage passwords. This method fails if the email is passed to another party but we don't think that will be a particular problem in practice, especially if CA references expire after a period.

We will want to be able to configure a blacklist of people/IP addresses and rude words.

4.9 Cookies

A cookie is a bit of information stored on the user's personal computer. We can usefully use that to recognise when somebody revisits. For example we can welcome them by name after looking up their record and tell what sort of user they are. We can also save the users personal preferences such as the way they last had their problems or jobs listed.

However cookies cannot be relied on because (a) they are often turned-off by the user or their IT department and (b) some people may use different physical computers.

Therefore we use them as a convenience tool to make life simpler for users rather than a necessity. The main access related use of cookies will be with Reporters where we may give them the option of having their password stored on their computer.

5 Operation

In this section we discuss how the system will be implemented and managed

5.1 Hosting

5.1.1 Suggested hosting configuration

a Dedicated server

Our preferred server configuration is a dedicated system which allows it to be tailored to the needs of the service.

b Package for main server

The sizing calculations in section 3 indicate that nothing exceptional is required to run the system. (But of course a badly tuned database will be orders of magnitude slower that a well tuned one which can clobber the most powerful or inappropriately matched hardware.) Therefore we propose the following package - or something like it for the main server.

Linux 'box' with dual processors 2Gb ram 20Gb disc
Apache web server
MySQL database
PHP web page scripting

c Mirroring for performance and backup

MySQL supports replication in real time which means

- We always have an up to date duplicate database
- We can share read-only database accesses to improve performance (a bonus which we don't anticipate needing to rely on.)

This requires a second computer which although configured as the main one does not need the same performance.

Because the system may contain safety-critical reports we want to make sure these are not lost. Data integrity is more important than 100% service availability. With a replicated database and a 'stand-by' server we can deal with unplanned maintenance of the main server and do planned maintenance at more convenient times accepting degraded performance.

d Electronic security

The server would be being used for a very limited number of services which makes it easy to strip out many possible security problems. There will be a handful of users which makes access control relatively easy. Nevertheless it may be appropriate to have a proxy acting as a gateway and firewall which if need be can be sacrificed to malicious attack.

e Physical security

While there is nothing of any particular intrinsic value we must protect against deliberate and accidental damage. Some sort of physical separation would seem to be indicated. However from the operational point of view we want both the main and the mirror to be co-located.

f Power supply

- Glitch and safe shutdown protection.
- In the event of lengthy outage we suggest it would be better to physically transport some of the equipment to an alternative location rather than invest in a stand-by generator.

g Communications resilience

Communications failures are one of the most common causes of service failure, and can take ages to sort out.

If the servers are on a single site, operating through a single telephone exchange, physical communications resilience is difficult to ensure. The answer is probably to physically move the servers to a fall-back location in this event.

The same strategy could be used to get to the bottom of other 'mysterious' communications problems.

A fallback ISP would be required.

5.1.2 Alternatives

There are many web hosting companies who could provide the appropriate platform for this system. Our concern would be lack of control over the details of configuration as described above. It would be prudent to have a stand-by hosted by another company.

5.2 Set up and test

5.2.1 HAs

We need to do some bare-bones populating of the HA table before being able to start. Once we have a reliable email address the completion and on-going maintenance of these details is the responsibility of the HA.

5.2.2 Localities

a Ordnance survey data

The Ordnance Survey has a Gazetteer which could be adapted for our use. This has about 10 times too many places though so considerable weeding would be required. (A very fine grained locality database is not a good idea as then what would happen is that a search for problems in and around a village X would not show problems in the locality "Jenkins Cottages" or "Five ash corner". The

The Ordnance Survey charges a significant licence fee which will have to be negotiated.

b D-I-Y

An alternative is to get Localities set up by HAs themselves. This would be something like 500 place names. (We suspect a little creative thought by a local IT bod should be able to generate.) There is no need for anything more than a place name.

While the D-I-Y method might appear to be inefficiently labour intensive, we think that this will be less so than weeding 9/10ths of an OS gazetteer.

c Choice of methods

Either method will require HAs to alter the data. This will continue as the system gets used and errors and omissions are found and clarifications need to be made. (For example it may be found useful to split a locality along the lines of "Fairstead (Except A18)" and "Fairstead(A18)" to separate Highways Agency matters.

The D-I-Y approach uses names as local people use them.

Although it might be seen as a disadvantage for HAs to have to start by investing time in creating their locality list, we pint out that the OS alternative would require more work and if ignores would swamp the public with localities which are more like locations.

Therefore we strongly recommend HAs compile and maintain their own lists of Localities.

5.2.3 Test data

A transactional system is generally tested by carrying out transactions rather than manipulating data so the emphasis should be on generating test cases which exercise the whole system (ie computer and human).

The training period described in 5.3 below will require periodic inputs of problem reports to be generated. We may provide a 'give me more' button so that users can generate suitable exercise data themselves. These test exercises will need to be parameterised so that for example a HA can generate test data that will go via a particular maintainer.

5.3 Training

5.3.1 Suggested approach

We propose a big-bang approach where the following events happen in the order listed:

- Pre-release testing and acclimatisation of system staff (Within NatPot)
- Release to *all* HAs with instructions for HA's preparatory work
- HAs given dummy example training problems to pass to Maintainers and thence Contractors.
- End of training period coincides with start of publicity - System goes live.

We are aware that getting local government to carry out such coordinated actions is like herding cats, nevertheless we feel that a patchy implementation of a *national* system isn't really a national system and would require much more chasing.

Obviously this would require some direction from central government.

5.3.2 Acclimatising system staff

In computer terms this isn't a large system but if it is to be run professionally then the operators need to be familiar with how it works and what to do if things go wrong. We anticipate administration will be in the order of half an hour a day of very routine matters. Therefore the problem is how to be sure that appropriate actions are taken in exceptional circumstances. The time to run through and document exception handling is before the system is released.

5.3.3 Trial period

This could be thought of as happening in two phases where the overall timescale is determined nationally but within that the HAs are in charge.

- Setting up local data (Own details, Maintainers and Localities) (1-man-day)
- Trying out the system using dummy problems.

It will be important to monitor progress in these phases. For example if in the first week a HA hasn't done any work on Localities that is a signal for management action. Similarly we would expect at least a dozen dummy reports per Maintainer by week two and an average of two job items per Contractor by week three. (The timings here are illustrative nevertheless a practical starting point.)

5.3.4 Materials

We feel that each user should not need a handbook beyond what appears on the web pages that they use. Once the purpose of the system is apparent there should be no difficulty following tasks through. Notice that as we go down the HA-Maintainer-Contractor pyramid so the number of options is fewer.

On the other hand HAs will need a road-map to tell them how to get started, how to publicise the scheme for locals to use, what data will be available and how to get more information. This will come from central government who have the necessary channels of communication already in place.

5.4 Routine administration

5.4.1 Server maintenance

Daily maintenance should be negligible.

Planned maintenance such as OS patches and upgrades can be tried on the backup server first. This requires standard server administration IT skills.

5.4.2 System maintenance

A working system is unlikely to need fixing urgently. Nevertheless there will be opportunities to tune the system in the light of experience. Standard change-control procedures apply.

5.4.3 Trapping service interruption

Experience shows that a fully functional system can become very slow or stop 'for unknown reasons at any time'. What we *don't* want is for users to phone up after a day or so and say 'by the way did you know the system is broken'. Therefore we want to monitor

- Are pages being served?
- Are pages being served at proper speed?
- Is the database working at proper speed?
- Can the server 'be seen' by the rest of the Internet?

To trap gradual deterioration we need comparable log statistics over a long period.

To trap interruptions we need an alarm and somebody to respond to it.

5.4.4 Dealing with urgent technical matters

Technical staff will need to be available on-call.

5.4.5 Dealing with suspected system abuse

Where heuristics indicate unusual user activities (eg people we know are Contractors adding problems as if they were Reporters) we should be passing this concern and evidence to HA auditors.

Where people abuse the system by

- posting abusive or inappropriate messages
- systematically probe the CA system
- trying to guess passwords

we will want to exclude them. (Note that the system sits between the parties so is in a position to filter all communications, particularly those relating to Reporters.) This will require some configuring of blacklists of IP addresses, people and rude words. Where reporters are involved with inappropriate posts we will have to tell them they have been barred.

5.5 System management activities

5.5.1 Usage monitoring

The quality of service can be quantified by measuring such things as response times and number of reports that needed clarification before they could be acted upon.

What is of equal significance is the amount of use the system gets. Of course perfectly maintained roads would result in negligible reports, but a more realistic assumption is that people don't know about the facility or have tried it and been disillusioned. The system can easily report on numbers of reports by HA and pass that on (in context) to HAs for their consideration.

5.5.2 Operations review

It is always appropriate to formally review operations periodically.   This would fall into two categories

- Current operations
- Future developments

with three scopes

- Technically providing the service
- Delivering what HAs and Maintainers want
- Delivering across the whole nation.

5.6 Project and quality of service delivery management

5.6.1 Project management

This isn't a complex project with many risky elements. The difficult bit will be timetabling the trial to coincide with launch publicity. Once these have been decided it will be difficult to alter the schedule.

The criteria for service delivery can be deduced from 5.6.2 below, while the tools used to provide some of the data required have been discussed above.

5.6.2 Quality goals

Quality Goals are principles which can be used to create specific objectives, steer design or development of management policies and systems.

a First implementation

- Planned and orderly introduction
- Technical, clerical and public matters are coordinated
- Works first time
- Nationwide implementation
- Publicity is appropriate

b Operation

- Well known site and easy to find
- Localities are the right size
- Confidentialities preserved
- Safety-critical matters are dealt with properly
- Escalation (complaints) work
- Non-maintenance matters are forwarded appropriately

c System performance

- Easy to use by public
- Communications go to the right places
- Clerical staff find it easy to use
- Web pages are served quickly even at peak periods
- Low maintenance overhead
- High level of system reliability

d System benefits

- Data on volume of defects is available
- Data on the way reports were dealt with is available
- Data on the mix of defects is available
- Public confidence and satisfaction is measured

6 Discussion

6.1 Success factors

Success factors are those matters which are under management control.

6.1.1 Preparation

a Design and analysis

Insufficient and inappropriate system design and risky assumptions probably cause the most disruption. There will inevitably be refinements as details become clarified but these should not impact on the overall structure of the system or project as a whole.

b Sizing

The development work required and the necessary IT equipment and configuration must be properly estimated.

c Coordination

The system development must be timetabled with a window of set up and familiarisation which is also coordinated with a public launch. These events are much less effective and result in enormous confusion if original schedules are abandoned.

d Realistic scheduling

6.1.2 Comprehensive approach

a Defining the system

It is a mistake to look at the IT system as an end in itself. The complete system also encompasses

- Making it work as a tool for improving the quality of roads
- Reducing clerical effort
- Encouraging the public to make reports

b Motivation and public relations

In theory we could let HAs ‘muddle through’ as they can’t ignore reports sent by email and if they don’t take advantage of a tool for doing it efficiently then that’s their problem. However a more sensible approach is for central government to explain what they are expected to do and when. This will form the basic for simple project targets along the lines of 5.3.3.

There is no point in creating this system if the public don’t know about it. Therefore a public relations campaign is required to inform the public about the system and how it will benefit them.

6.1.3 Sufficient funding

a System development and operation

Insufficient funding will result in an unreliable system caused by poor quality programming, lack of testing. Furthermore the majority of the on-going costs will be spent on ensuring quality of service.

b Local government

We don't expect this to be funded as the clerical savings will pay back the investment of time.

c Public relations

There will be two strands to this:

- Local - Councils putting articles in their magazines - No special funding
- National - A proper campaign requiring a budget

d Further development

It is the nature of this sort of system that people discover possibilities as they get used to it. Some improvements can be achieved quickly and cheaply on-the-hoof. We would expect a component of the operating fees to be assigned to minor developments. This avoids the situation where absolutely nothing can be done without a lengthy decision making process.

6.2 Failure factors

Failure factors are issues which are outside management control but for which contingency planning may be required.

6.2.1 Unexpected supplier failure

a Initial development

This risk depends on the resilience of the *development team* and quality of programming methods rather than the size of the firm doing the work. Obviously there is less opportunity for things to go wrong over a shorter development period.

b Ongoing operations

We prefer the small-but-dedicated model of operations to the general bureau one. This means better control of operations and management. In any event a supplier failure is a possibility and a contingency plan is required. The supplier might fail financially or fail to provide the necessary facilties.

6.2.2 Wholesale rejection by HAs

This will require further prompting by central government to overcome resistance to change, but the system has been designed so that problem reports cannot be ignored without them becoming obvious. Also the system cannot be bypassed as the reporter's contact details are not passed to the HAs.

6.3 Preparing HAs and maintainers

We have discussed this above. The important thing is for central government to establish a timetable and explain what HAs have to do and when and how it will be up to them to get the pyramid of Maintainers and Contractors to cooperate.

6.4 Measuring results

6.4.1 Public satisfaction

a Use

Collecting usage statistics is easy. Putting these into context is a bit more difficult in that HA areas have different characteristics.

b Opinions

We have built-in a facility for Reporters to respond with how well they consider the problem has been dealt with. Public satisfaction in this area is important because (a) that's what they pay their taxes for and (b) it will encourage them to use the system again and save money or an accident as a result.

6.4.2 Statistics

a Compared across HAs

The responsibility for maintanance lies with HAs. This is the appropriate classification for comparison. Although most of the data collection will relate to the way Maintainers operated it will be aggregated for public use (although see 6.4.2.c below).

While HAs have areas with differing characteristics, the general levels of performance should be comparable. ie. A 'dangerous pothole' should be fixed in the same time in the city and the country.

League tables are an obvious output which is easily understood. However for these to be useful, rather than being just another stick taking resources away for what really matters the measures used should reflect things which are worth measuring. For example a larger 'number of reports' doesn't necessarily mean the roads are in a dreadful state, while an increased ratio of serious to all defects reported probably does indicate a policy of neglecting all but the most serious cases.

A benefit of a single national system with identical reporting classifications is that data across HAs is automatically comparable. Intelligent use of these statistics can be used to drive up quality of service.

The system will collect satisfaction levels which is a 'soft' measure of how well matters are dealt with. We may be able to refine this in order to separate

- How quickly the Maintainer reacted
- How well the Maintainer 'fixed the road'
- Whether the Reporter thought the Maintainer acted reasonably

b Compared across time

The same figures as for 6.4.2.a but showing improvement or deterioration.

With large amounts of data it may be worth looking at monthly performance to investigate seasonal variations.

c Management information for HAs and Maintainers

While outsiders want to know 'the bottom line', managers need more detailed information. HAs can compare Maintainers and Maintainers can compare Contractors. These figures (such as for example Time a Contractor takes to respond to a Job Item) may not be strictly comparable but in the management context can be used for useful measurements.

d Analysis

We have not specified the exact analysis of basic routine statistics, preferring to leave that to a management-driven exercise.

The system will collect a large database of instances to draw on for in-depth analysis. For example we might think it was a good idea to investigate the relationship between complaints concerning failure to do anything and 'what happened next'. This type of investigation can be used to support management policies.

6.4.3 HA and Maintainer satisfaction

As we have mentioned several times HAs and Maintainers don't have much choice but to interact with the system. Nevertheless there may be opportunities to improve awkward aspects of the system and increase its usefulness to HAs and Maintainers. Therefore we would anticipate soliciting feedback.

6.4.4 Outside objective measures

The overall purpose of this system is to improve the state of the roads. In doing so there are other benefits. Can any of these be measured with enough accuracy, and is it worth doing so to prove a 'before and after' improvement? We suspect that there are too many external factors.

6.5 Extending the system

6.5.1 Maintainers using the system for all defects

An obvious extension which we forbid at present due to the potential for serious fraud and massaging of statistics is to allow Maintainers to create problem reports on the system themselves. To implement this would require:-

- Better identification of individuals
- Being able to separately identify in-house reports
- Logic modifications
- A code of practice

If this extension was to take place then a proper systems analysis exercise would be required to investigate the appropriate scope of the clerical procedures and 'hooks' into other management systems.

6.5.2 Ask reporters after a year if remedial action was successful

While the system as-designed offers Reporters the opportunity to say how well they think the issue has been dealt with, there is no long-term follow-up. It is very common to find repairs failing within a year, with signs to that effect visible in much shorter periods. Therefore to monitor this sort of problem it may be useful to ask the original reporters with their local knowledge, after say a year, if the action taken has lasted. This would be easy to add.

6.5.3 Other highway related issues

The scope of this system is all highway *maintenance* issues. This includes footpaths, bridleways, cycle tracks, failed lighting, excess vegetation, blocked drains and wrong signs as well as potholes in the road.

However this is restricted to the cases where there is something defective rather than where something could be better. There are cases where say a sign is definitely wrong but it needs to be improved or altered rather than 'fixing it'. This split arises through institutional arrangements for splitting maintenance activities from capital projects and from the point of view of the general public who want better roads is artificial.

The system as-designed allows a maintainer to pass the buck to a non-maintenance '3rd party' and that's the end of the matter with 3rd party and Reporter communicating directly off-system. (Although the reporter might post the 3rd party replies to the comments section of the problem and raise it as a complaint.)

It is worth investigating how the system might be extended to encompass 'we want a 20mph zone' and 'I object to your plans for parking restrictions'. Potentially this a very large field which may be developed as a natural extension of this system. But we repeat that investigation is required after the current system has been established and proved reliable.

A Cryptic Access(CA) - Obfuscating access IDs

Problem

We will have a combination of users that are not explicitly authorised (because the overhead of managing authorisations is too high) and web pages that are accessed by parameters included on the command line. This presents a problem of impersonation. For example if user number 123 receives an email with a link in like:

`<http://www.natpot.co.uk/yourdetails.php?userid=123>`

there is no protection against someone trying out different numbers to look at and perhaps alter other user's details.

Actually we do expect a degree of checking that the user seems to be who they say they are, but in order to make it simple enough for general users we can't insist on methods which are difficult to break. HAs and maintainers *will* require authorised logins, reporters and contractors *won't*.

Scope

The IDs to be protected in this manner are:-

- Reporter
- HA
- Maintainer
- Contractor
- Job/Job item

Objective

To prevent impersonation we want to do two things:

1 Make it *difficult* to find *any* other ID by poke-n-hope
2 Make it *very difficult* to find *a particular* ID

Options

There are two approaches which we can use in order to hide this information:

- Fixed mapping
- One-time page reference

Fixed mapping

The simplest method is to have a fixed mapping from ID (plus salt) to a hash. The size of the hash determines the difficulty of finding IDs at random.

ID = 123 might become hash A458CC8DB223

(In this example a 48 bit hash for say 200K reporter IDs gives about a 1 in 1000 million chance of finding any ID.)

However this scheme does not protect against leakage of the hash itself which is quite a likely event given that these will appear many times in emails which are easily replied-to and forwarded. This means that our second objective is not likely to be met.

One-time page reference

In this scheme the system works out what the full command line would be, remembers that and gives it a random number. That number is then passed out by email. When the email link is used it supplies the random number to the system which retrieves the actual command line.

For example suppose we want to tell a user how to access their details. The command line parameters might be `?user=123`. The system generates a unique random number, say of 64 bits and stores this on its database. Now it knows that if it receives a command line with say `?ref=5418202761023` it must reconstitute the real command line by looking it up. In the meantime in this email the embedded link looks like `<http://www.natpot.co.uk/reply.php?ref=5418202761023>`.

This scheme means that if an email should be leaked it will only give access to this single screen.

The lifetime of most of these emails will be a few days. Also it will be possible for users to get to the place they want by stepping through the screens to get to the specific page if the look-up has expired. Therefore we can set an expiry of say two weeks on these lookups. A shorter expiry reduces the risk from leaked emails being used. Perhaps we should provide a variable expiry date.

It would be possible to remove all references by reverse lookup , say all those with a command containing “user=123". This wouldn’t block a user from legitimate use but would invalidate all references used in any leaked emails.

Discussion

The overhead of a few table accesses to uniquely identify a screen with complex parameters and the best security options we can expect seems reasonable.

Say we create 4000 emails per day each with 4 links and we leave all references live for a month this gives a table with 480K records. (Possibly 20Mb in size.)

The command line interface has two characteristics

- It is ‘clean’ but completely obscure
- Bookmarking the active link will fail after the look-up expires

The latter may will require a little bit of user education. (Bookmarking an actual web page once the command line has been reconstituted will work.)

However, even with page references being encoded with the one-time system we *still* have the problem of IDs being visible while on the page. (We need this if users are going to be able to bookmark pages which we expect them to do quite a bit with some of them - eg Contractor Xs list of outstanding jobs.

So we *also* need to use the fixed mapping scheme (hashing IDs) to prevent contractor number 123 simply changing the 123 to something else to see what jobs the others are getting.

Conclusion

- Use a One-time page reference system in emails.
  and
- Use ID hashing