

Safety-Critical Systems: Open Assessment 2001-2002

Prof. Chris Johnson,
University of Glasgow, Glasgow, G12 8QQ. Scotland.
johnson@dcs.gla.ac.uk, <http://www.dcs.gla.ac.uk/~johnson>

1 Introduction

Incident reporting systems gather information about near-miss occurrences and adverse events. They are used in many different industries. For the purposes of this assessment, we will be focusing on incident reporting for medical devices.

2 Your Task

Your task is to design and implement a web-based system for the analysis of medical incident reports involving software failures. The US Food and Drug Administration's on-line search tool returns more than 500 records for software related failures in medical devices. Clearly, this mass of information needs to be filtered in some way. The most obvious criteria to sort this data might be by class of devices. This would indicate whether some forms of equipment posed a higher risk of failure than others. Alternatively, you system could show incident frequency per manufacturer. This might be used to support arguments either in support of Perrow's Normal Accident ideas or Sagan's views on high-reliability organisations. The way in which you filter the data is entirely up to you but you must justify your decision in the documentation (see below). This justification should refer to the material that has been covered in the lecture component of the course.

At present, most incident reporting systems provide standard database facilities. Some also support free-text information retrieval techniques. The results of queries are then used by statisticians and analysts to manually produce tables and graphical overviews of incident trends. This can be expensive and is also error-prone. I would like you to automate part of this process. For example, you might write a programme that automatically generates a graph of the frequency data mentioned in the previous paragraph. Alternatively, you might choose to implement one of the more dynamic visualisation techniques being explored by Fraser Speirs for UK railway incidents ¹.

In the following paragraphs, I will describe a dataset that you can use to drive your visualisation. This data is unlikely to be in a format that can be directly used by your visualisation. You should, therefore, either develop tool support to convert the existing data into an appropriate format. Alternatively, if you are short of time it is acceptable to manually convert some of the data and then describe how a tool might automate this conversion in the future.

3 The FDA's MAUDE System

We will be using data from the FDA's Manufacturer and User Facility Device Experience Database (MAUDE) system. There is a searchable interface that can be used to rapidly extract information about previous incidents. The entire dataset is also on-line. This is divided into several formatted files. Each file contains information about a particular relation within a relational database schema. Fortunately, there is a guide to the analysis of this data so if you have the time to automate data extraction then this can be done. I can provide some guidance with this - email me if you are interested:

¹See <http://www.dcs.gla.ac.uk/speirsfr/papers.html>

- Overview of MAUDE,
<http://www.fda.gov/cdrh/mdrovrvw.pdf>
- Interface to the MAUDE database,
<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM>
- Source data and description of fields, <http://www.fda.gov/cdrh/maude.htm>
- Verity Free-Text Retrieval System
<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Verity-help.cfm>

Your system should enable users to more easily obtain the statistical and other information that is disseminated by publications such as the FDA's User facility reporting Bulletin. Issue 18 in the following index is a good one to start with:

- User facility reporting Bulletin Index:
<http://www.fda.gov/cdrh/fusenews.html>

Here are some other useful links both on the importance of medical incident reporting and on the reporting of device-related incidents within the UK NHS:

- The Institute of Medicine Report 'To Err is Human':
http://stills.nap.edu/html/to_err_is_human/
- The UK NHS 'Organisation with a Memory' Report:
<http://www.doh.gov.uk/orgmemreport/index.htm>
- The UK Medical Devices Agency:
<http://www.medical-devices.gov.uk/>

Before starting to implement anything, I would recommend reading 'To Err is Human' and 'Organisation with a Memory' to get some idea of the context in which incident reports are submitted.

4 The Design Brief

This exercise enables you to apply the knowledge that you have gained about safety critical systems development. Your primary aim is to demonstrate the effective use of incident data to support an argument about the causes of software failures. In the documentation (see below) that you submit with your solutions, it is very important that you explain who the users of your system will be. You must also specify the particular information needs that the site will support.

5 Assessment Criteria and Submission Details

This exercise is degree assessed. It contributes 30% to the total marks associated with this course. The body of the report should not exceed fifteen A4 pages. The report must be printed out and must be submitted in a secure binder (i.e., one that will keep the pages together and in the correct order). It must include:

1. A title page containing your student as well as your contact details (email address etc);
2. A table of contents and appropriate page numbers;
3. A section on the design of the system. This should include some consideration of alternative approaches and a considered justification of the reasons why you build the system in the way that you did.

4. An implementation section. This should describe the techniques that you used during the development of your system.
5. An evaluation section. This must consider both formative and summative testing. Formative evaluation might include user testing of pencil and paper prototypes and of partial implementations. Summative evaluation describes the testing of the final system.

In addition to the fifteen pages associated with the body of the report, you may also include appendices. These should contain the listing of any code used during the implementation together with suitable acknowledgements for the source of code that has been borrowed from other programmers. They should also provide any internal documentation (maximum two sides). These are notes that are intended to provide guidance for anyone who must maintain or develop your system.

Your solution should be handed in at the start of the lecture on Wednesday 12th December 2001. Extensions will only be granted in exceptional circumstances and they should be requested prior to the deadline. Extensions for medical reasons should be reported as soon as possible and should be supported by forms from a medical practitioner. Extensions for equipment failures may be granted provided that you let me know as soon as they occur; so that I can make sure they get fixed as soon as possible. Please make sure that you keep back-up copies of all of your work towards this exercise.

The following marking scheme will be applied:

- 15 for the design;
- 15 for the implementation;
- 10 for the evaluation;
- 10 for the technical documentation.

All solutions must be the work of the individual submitting the exercise. If any code or design ideas are borrowed from course notes, books or other students then those sources **MUST** be clearly acknowledged. All questions about this exercise should be addressed to Chris Johnson.