Performance Standards and Test Procedures for Environmental Data Management Software

Martin Lloyd

Dr M H Lloyd, Farside Technology Research / SIRA Environmental Ltd
12 Acorn Industrial Park, Crayford Road, Crayford, Dartford, Kent, DA1 4AL, UK
martin.farside@btinternet.com, +44(0)118 941 2728

Abstract- Environmental regulators must have confidence in the complete measurement sequence: from sample point to measurement report. Thus, they need to be confident not only in the measurement instruments that acquire the data but also in the data management software that processes, stores, and prepares reports. This paper describes a new data management software standard for the UK Environment Agency's MCERTS scheme, which hitherto has only covered instruments. Our approach divides the standard into three parts: the generic quality of the software, which is not addressed here, because it concerns software engineering; the generic features of data management; and the application-specific features, referred to here as the 'sector standard'. We focus on generic data management: the need for a mathematical specification of any signal processing and calibration; auditability and traceability; and reporting. We have used the standard to conduct audits of data management products; these audits and feedback from diverse industrial bodies who have reviewed the standard, together indicate that it is appropriate for the certification of environmental data management applications.

Background

Computers are now an integral part of how environmental data is generated, stored, manipulated and reported. Problems with data management can have a number of serious adverse effects on its usefulness to inform decision making:

- affect the quality of measurements as they are made (or input into the data system);
- corrupt data which has been gathered;
- apply inappropriate policy or technical judgements, for example in the context of applying a model, where limits to key model parameters have to be respected;
- remove data from its 'natural' context, that is, to use data without reference to: the chemical analytical methods used, the measurement uncertainty, the detection limit, the definition of what 'zero' means, etc
- apply secret or obscure manipulations to data;
- make data management overly cumbersome and time consuming;
- make data management unnecessarily expensive;
- otherwise handle or present data in a way which does not accurately and constructively inform decision making.

To avoid these problems the UK Environment Agency has instituted a standard for data management applications software that fits into the UK's well known MCERTS (Monitoring Certification Scheme). This paper describes the rationale for the new standard. The author of this paper is the principal author of the new MCERTS standard.

Areas of Application of the MCERTS Standards

The Environment Agency established its Monitoring Certification Scheme (MCERTS) to deliver quality environmental measurements. The scheme is based on international standards and provides for the product certification of instruments, the competency certification of personnel and the accreditation of laboratories. Basically, the measurement devices, the people, and the software involved in making environmental data available to the Environment Agency must all reach a certain standard

We present the principles underlying the performance standards and test procedures for validation of software used for processing monitoring data from: water treatment and distribution; waste water treatment; emissions to the atmosphere, etc.

Product Certification

The UK MCERT Scheme for environmental data management software provides a formal approach to the product certification of environmental data management applications conforming to these standards. Product certification under this Scheme comprises:

- Audit of the software development lifecycle by an independent software specialist with expertise in this domain and MCERTS experience.
- Audit of the application software by the software expert using the criteria laid down in this MCERTS standard.
- Independent review of the audit report
- In the event of a successful audit, issue of the MCERTS certificate to the developer of the environmental data management application.

Scope of the MCERTS Environmental Data Management Standard

Organisation of the Standard

The standard is in three parts as shown in the diagram below:

- Part A covers the generic quality of the software and defines a standard for the lifecycle used to develop and maintain the data management application.
- Part B covers the performance of the environmental data management application (the "application standard").
- Part Cx covers the sector specific aspects of the application for sector x, so there are sector standards C1 – Cn, each contains requirements that are additional to those in Part B.

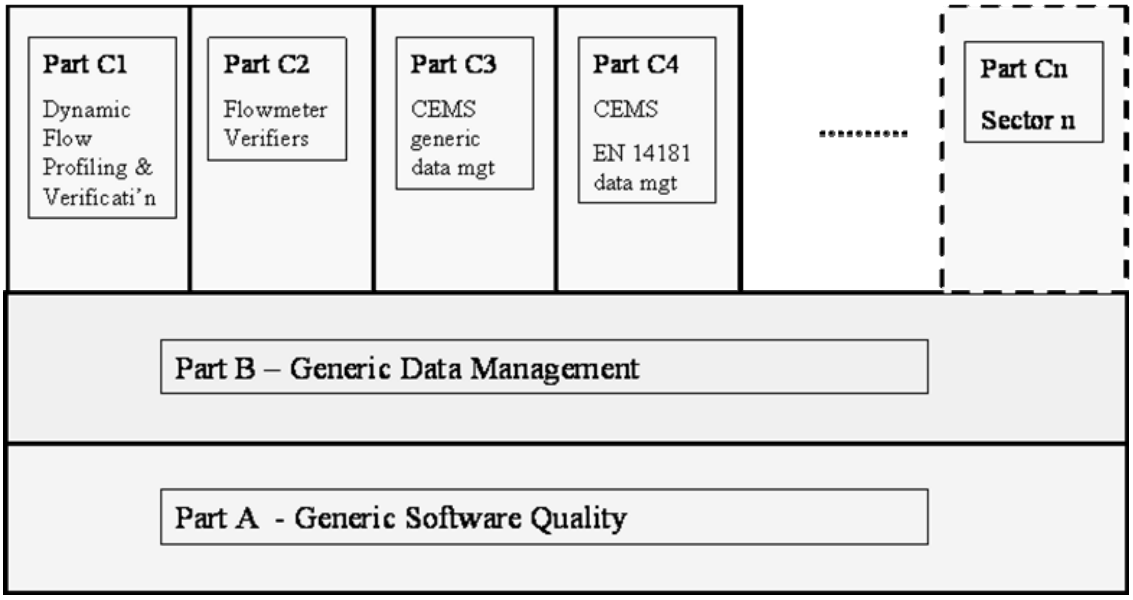

Figure 1 Organisation of the MCERTS Standard

The reasons for splitting the standard into three parts are:

- A number of software quality standards exist already and it is possible that some data management applications submitted for MCERTS certification may already have had their software quality assessed, in other words they may already comply with what we identify as Part

A of this MCERTS standard, for example safety-related applications complying with IEC 61508 [1].

- There are a number of generic data management requirements that fall naturally into Part B, that is, they are common to most monitoring data management applications.
- Discussions with suppliers of various environmental monitoring applications have shown that there is a diversity of application sectors with specific requirements. Moreover, it can be expected that additional ones will arise as the market develops. Hence we introduce a Part C standard for each significant sector.

Part C Sector standards

So far the following sector standards have been identified:

- C1 – Dynamic flow profiling and verification applications in the water industry;
- C2 – Flowmeter calibration verifiers ('Verifier Applications');
- C3 – Continuous Emissions Monitoring Systems (CEMS) Data Management applications, generic items
- C4 - Continuous Emissions Monitoring Systems (CEMS) Data Management applications, items relating to the EN 14181 standard.

We expect to add further Part C sector standards as required.

How this work contributes to the State of the Art

The MCERT scheme was introduced into the UK in order to improve the quality of environmental measurements reported to the Environment Agency. So far the scheme has concentrated on instrumentation. Now, with a growing number of software applications there is a concern that the integrity of reporting can be compromised by poorly engineered or misapplied software. This standard therefore seeks to combine the principles of good environmental data management with those of software engineering in a way that does not discourage the development of good quality products by the many small firms that operate in the environmental sector. This standard is a synthesis of ideas from a number of areas.

Methodology

Our approach has been to:

- Check the state of the art to see whether any equivalent standard exists
- Solicit opinions from trusted industrial observes as to the sectors most in need of standardisation
- Assemble a team with expertise in environmental data management, software engineering and the MCERTS standards. Each member is required to have strong knowledge in two of these fields
- Produce a series of drafts that are reviewed by the Environment Agency and selected industrial experts
- Test the final draft on two or three 'pilot audits' where companies with data management products are seeking certification for them and have volunteered to act as guinea pigs in order to test the effectiveness of the new MCERTS standard
- Revise the draft standard in the light of experience and release it for wider use

We also recognise that different application sectors will emerge. This is why there is a Part C that can be augmented by new sector standards.

Part A – Generic Software Quality

We do not report the software engineering aspect of the work in this paper because our main concern is with the environmental monitoring aspects of the standard.

Part B – Generic Data Management

In this part of the standard we try to identify the qualities that are common to most environmental data management applications. We only have space for a few points so after listing the main topics in Part B we select just three for more detailed treatment. Thus, Part B covers:

- Application documentation
- Mathematical specification and the processing of measurement data (standard paragraph B3)*
- Traceability and auditability of data (B4)*
- Storage and security of data
- Interfaces to measurement devices
- Report generation and the display and presentation of data (B7)*
- Confirmation of the certification of new versions and the withdrawal of defective versions
- Software installation and acceptance
- Commercial status of the supplier

Mathematical specification and the processing of measurement data (B3)

B3.1[1] The application developer shall produce a specification of the algorithms used by the application to process the measurement data. [2] insists that this document be produced and this standard follows suit for the same reason: all steps in the processing of measurement data have to be carefully specified and their associated sources of error identified.

B3.2 The Mathematical Specification shall include:

- Specification of numerical inputs and their ranges, their validation, and the handling of outliers.
- Definition of all formulae and specification of the algorithms used in the application, including their limits of validity and evidence of their suitability in numerical analytic terms.
- Use of stable formulae whose solution is not vulnerable to rounding errors.
- Validation of any non-trivial algorithms by means of an offline implementation using representative test data.

For example, the mathematical specification must demonstrate:

- The appropriate use of any floating point arithmetic and the avoidance of bad practices such as cancellation, division by very small quantities, exact comparison of floating point numbers, etc.
- The use of well conditioned formulae where small changes in the input data do not cause relatively large changes in the solution.
- Appropriate use of any scaled integer arithmetic.

In software engineering parlance, the mathematical specification typically forms part of a requirements specification.

During application software validation the results of the above off-line validation of non-trivial algorithms will be used to corroborate the results from the on-line version. It is very important that any test data sets and test software are as carefully designed and controlled as the main application.

B3.3 The Mathematical Specification shall specify how instrument status information is to be used (when it is available). If any of the following data are available then the application shall make use of it:

- Measurement uncertainty and/or device statuses returned by measurement devices.
- Indications of the validity of measurements based on the status of the measurement devices and measurement uncertainties computed within the application.

The principle is that, where possible, useful status information should not be ignored but used to indicate the validity of measurements.

[1] 'B3.1', etc identify the clauses in the standard.

B3.4 All input data shall be verified before being used in calculations, reports, displays or other application outputs. The principle is that unverified data must never be used in any output from the application. However, if the application receives data from another system that has already verified the data and marked it as such then there is no need to repeat the verification.

B3.5 Each measured value shall be accompanied by an indication of its validity, if the measured value is invalid then the reason for the invalidity shall be recorded. All conditions that can render one or more measured values invalid shall be recorded with the measured values. The method of recording shall permit the affected data to be identified, together with the reason for their invalidity. Note that the ability to recover this information from historical records is an important part of establishing an audit trail for performance of the application. The data processing shall use this information to determine which measured values are eligible for inclusion in the calculated values and reports.

Traceability and auditability of data (B4)

B4.1 Measurement data records shall be traceable to the physical location and time of the measurement, the measurement devices used, and the statuses of the devices.

B4.2 The time and date of measurement shall use UTC (Universal Coordinated Time) and shall normally make use of an independent time and date source. If such a source is not used then its non-adoption shall be justified in the application design. However, the non-adoption of an independent time and date source would be justifiable in a simple stand-alone application that is running on one PC and which is responsible for the time-stamping of all its input data and where the application timing requirements allow a margin of error on the time of day that is used. Networked systems or applications using data from several different input devices that time-stamp their data shall use an independent time and date source.

B4.3 The status history of measurement devices shall be held so that measurement data can always be traced to the operational status of the device (if available) at the time of the measurement. If the calibration of the device is traceable to a standard then a reference to that information, or a similar indication, should be included in the operational status. This illustrates the principle that measurement instrument status shall be readily traceable to a standard.

B4.4 All measurement data records shall be auditable so that the original input data and all subsequent modifications can be identified.

B4.5 All manual changes to data shall be auditable and traceable to the date, time, and operator responsible for the change. For example, a measurement database must be protected from attempts to export data into a spreadsheet application, to change the data, and then to import the changed data back into the measurement database. If such an operation is performed on database records then this fact must be logged and must appear in any audit trail pertaining to the custody of the measurement data. The principle that applies here is ‘no secret manipulation of data’.

Report generation and the display and presentation of data (B7)

B7.1 All reports and displays shall indicate whether any measurement data or calculated results are based on invalid or incomplete data. An example of incomplete data would be an average measured value taken over fewer points than normal because an interface has been temporarily out of use.

B7.2 Statutory reports and displays shall be labelled with their official title.

B7.4 Only reports generated by MCERTS certified applications shall be marked as ‘MCERTS compliant’ reports. Reports generated from exported data on other applications shall be marked as ‘Advisory’. MCERTS compliant reports will normally be identified by their official title in the header and be marked with the MCERTS logo.

B7.5 Export of reports and displays shall not cause validity/invalidity information to be lost.

B7.6 Where test data is used to exercise the application any displays or reports containing such test data must be unambiguously marked to indicate that test data is being used.

Results and Discussion

At the time of submitting this paper we have early results from our pilot audits of environmental data management applications. Already though, it has become clear that different sectors have responded in diverse ways, for example:

- Flowmeter calibration applications covered by Part C1 are a very active area as are continuous emissions monitoring systems, including EN 14181 compliant applications
- The committed interest of regulatory bodies like the Environment Agency is vital to the successful dissemination and use of the standard
- A lack of input from industry can seriously delay the progress of the standard
- The development of quite complex software applications by engineers who are not primarily software engineers raises the need for education and training in good software engineering practice
- There is much value to found in transferring good measurement software practice [2] – [4], from metrology applications to those in the environmental sector.

We anticipate wider use of this standard as the number of sector standards grows.

Results from Continuous Emissions Monitoring Software Applications

The audit process has had a significant effect on the company who develops and supplies this software. The most obvious improvements are:

- Using Part A has already led to a marked improvement in software engineering methods and the adoption of more powerful tools for managing and testing this application software
- Using Part B has uncovered areas of weakness in the application and in the methods used to support end users in the field. Strengthening the areas of weakness has led to a reduction in software defects, as well as an increase in their early detection.
- The pilot application combines both Part C3 (CEMS) and C4 (EN 14181) functionality. The audit has provided a further objective check of the compliance of the software to the European norm.

As the development of the standard has progressed, interest from suppliers to the environmental industry has increased, as well as from regulating bodies like the Environment Agency. Further audits are being planned in other industrial sectors and additional sector standards are being considered.

Conclusions

This MCERTS standard attempts to combine the disciplines of environmental data management and software engineering. Experience so far shows that it has been a very useful investment of time and money.

References

[1] “Functional Safety of electrical/electronic/programmable electronic safety-related systems”, *European Standard 2001 IEC 61508*, 1998 + corrections 1999

[2] Brian Wichmann, “Software Support for Metrology Best Practice Guide No 1, Measurement System Validation: Validation of Measurement Software”, *Version 2.1 Draft 4, NPL Report*, July 2003.

[3] “Software Support for Metrology Best Practice Guide No 12, Test and Measurement Software”, *NPL Report*, October 2002.

[4] Roger Barker and Graeme Parkin, “Techniques for Validation of Measurement Software – without specialised tools”, Report to the National Measurement System Directorate, DTI, London, March 2004