

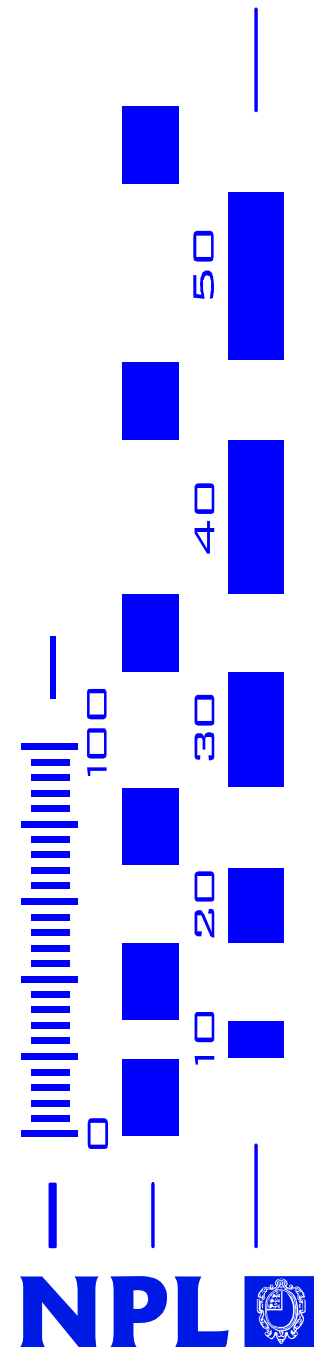
**Presentation to: Gamma Radiation
Spectrometry Forum**

Validation of Measurement Software: SSfM Best Practice Guide No. 1

Graeme I Parkin

Graeme.Parkin@npl.co.uk

Date: 3 December 2002



Aims

- ◆ To describe how the guide *Measurement System Validation: Validation of Measurement Software* can be used to produce software of a certain quality

Content

- ◆ Describe the guide: *Measurement System Validation: Validation of Measurement Software (MSV)*
- ◆ Outline IEC 61508
- ◆ MSV with IEC 61508
- ◆ Outline current Project
- ◆ Future

MSV guide

Aims:

- ◆ Users
- ◆ Suppliers

MSV guide continued

Two parts:

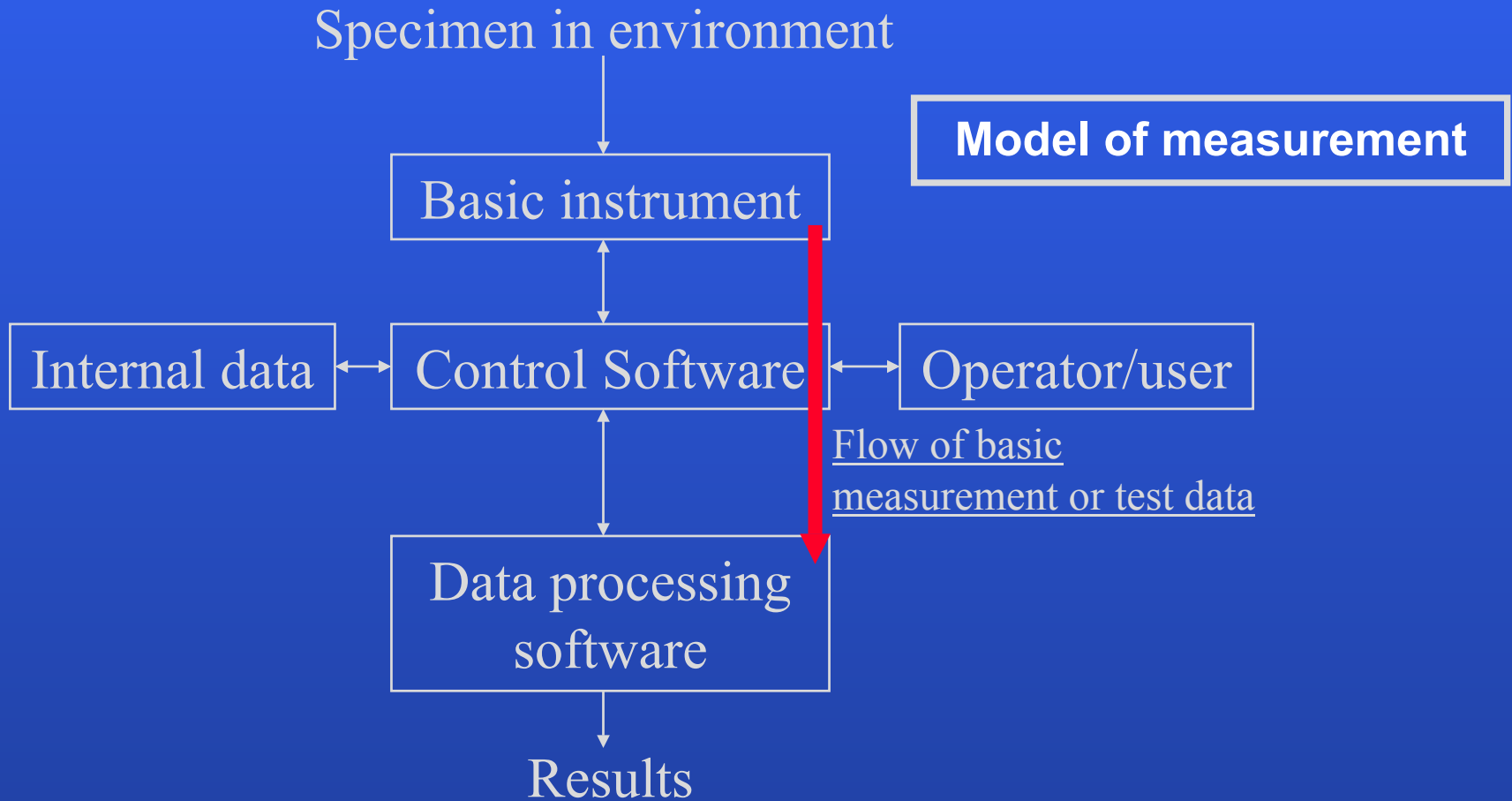
- ◆ Management overview
- ◆ Technical application

MSV guide continued

Four stage process:

- ◆ Analysis of the physical process
- ◆ Risk assessment
- ◆ Determine the integrity required for the software (Measurement Software Level)
- ◆ Guidance on the software engineering methods to be employed for the particular Measurement Software Level (MSL)

MSV guide continued



MSV guide continued

Risk assessment is based on the following:

- ◆ **Criticality of usage – critical, business-critical, potentially life-critical, life-critical**
- ◆ **Legal requirements – specific measures**
- ◆ **Complexity of control – very simple, simple, modest, complex**
- ◆ **Complexity of processing of data – very simple, simple, modest, complex**

MSV guide continued

Measurement Software Levels 0, 1, 2, 3, 4 are determined by:

- ◆ Software issues: end to end, raw data testing, history, errors, control (false results), operator interface; and
- ◆ Risk assessment values selected

MSV guide continued

From the Measurement Software Level you then:

- ◆ Meet ISO 9001 requirements
- ◆ Apply recommended techniques for the level selected

IEC 61508 Outline

- ◆ Functional safety standard
- ◆ Generic – instantiated for application areas
- ◆ System
- ◆ Covers whole life-cycle

IEC 61508 Outline continued

Seven parts:

- ◆ Part 1: General Requirements
- ◆ Part 2: Hardware
- ◆ Part 3: Software
- ◆ Part 4: Definitions and Abbreviations
- ◆ Part 5: Examples of methods for the determination of safety-integrity levels
- ◆ Part 6: Guidelines on Part 2 and 3
- ◆ Part 7: Overview of techniques and measures

IEC 61508 Outline continued

- ◆ Has SIL 1, 2, 3, 4 (but more Quantitative than Qualitative)
- ◆ SIL for software can only be Qualitative
- ◆ Less prescriptive in terms of techniques to use

IEC 61508 Outline continued

SIL	High demand rate (failures per hour)	Low demand rate (failures per demand)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$
Safety integrity Levels		

MSV with IEC 61508

- ◆ Only measurement software
- ◆ Levels map onto one another (SIL 1 -> MSL 1 etc)
- ◆ Clear which are IEC 61508
- ◆ Selection of techniques for each level to meet the requirements of that level
- ◆ Audit check lists
- ◆ Traceable to IEC 61508

MSV with IEC 61508 continued

Techniques selected for MSV:

- ◆ Only interested in software
- ◆ Are being used widely
- ◆ Can be audited
- ◆ Some combined together
- ◆ Allocated to a level
- ◆ Some alternatives

MSV with IEC 61508 continued

Techniques in the guide but not in IEC 61508:

- ◆ Regression testing
- ◆ Accredited testing
- ◆ Numerical stability
- ◆ Mathematical specification
- ◆ Numerical reference results
- ◆ Back-to-back testing

MSV with IEC 61508 continued

Potential problems:

- ◆ SOUP
- ◆ Use of a safety case
- ◆ Dependence on development
- ◆ Validation methods not covered in this guide
- ◆ Complexity versus reliability

Current project – Software support for Metrology (SSfM) – DTI

Consists of:

- ◆ NPL – Technical content
- ◆ Adelard – Review with respect to IEC 61508
- ◆ SIRA – CASS (Conformity Assessment of Safety-Related Systems) acceptability

Current project (SSfM – DTI) continued

Validation of the guide:

- ◆ Review by Adelard, SIRA and open for public comment
- ◆ Audit visits

Current project (SSfM – DTI) continued

Progress:

- ◆ Draft version available for public comment since end of October 2001 (SIL1, SIL2)

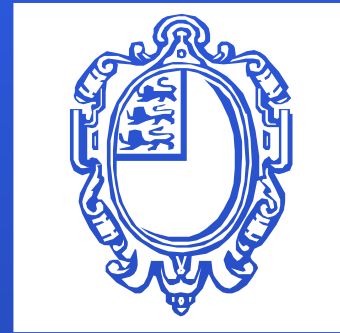
- ◆ See:

http://www.npl.co.uk/ssfm/download/#ssfmbpg1_draft

Future

- ◆ Will be extended to deal with SIL 3
- ◆ Acceptability to CASS
- ◆ Extend to IEC 61508 SIL 4 (MSL 4) – requires more funding
- ◆ International status

NPL



National Physical Laboratory

SSfM

3 December 2002

Gamma Radiation Spectrometry Forum

Slide 23

NPL
National Physical Laboratory

