SAFETY CRITICAL SOFTWARE IN PROCESS CONTROL AND NUCLEAR POWER

D Welbourne
(Formerly with NNC Ltd, Booths Hall, Knutsford, Cheshire WA16-8QZ)

The uses of computer systems on nuclear plant are outlined, with comments on the use for process control. The development of safety-critical and safety-related uses are described. For nuclear power, these are classed as Category A and Category B with C by the International Electrotechnical Commission (IEC), in Standard IEC1226. The key application and reliability requirements are given, with the standards relevant. The draft standard IEC1508 is discussed. Comments are given on acceptance by the nuclear safety regulators and the consequences on system structures. Expected developments in computer use are discussed, with special reference to Eastern Europe.

Key words: Standards, soft control, safety-critical, software, reliability, research and development, safety, safety-related, nuclear, nuclear power, control, protection, integrity, classification, faults, hazards, diversity, PWR, VVER, AGR, CANDU.

THE EARLY USES OF PROCESS PLANT COMPUTERS

The early systems on process plant used redundant minis and input/output equipment. Typical overall outage times of about ten hours per year were achieved when applied to nuclear plant. They displayed groups of signals on VDU screens, initially in monochrome. Alarm lists were shown in chronological order, and also sorted by plant area. Alarm logic was included, sometimes incompletely, to attempt to handle the floods of alarms which appear at major plant trips. Records and logs were made automatically. An early report of the International Electrotechnical Commission (IEC) was published as IEC643 (1) for nuclear plants and gives the basic functional and performance requirements for such systems. These functional roles are still very important, and continue to grow.

It was soon apparent that the system designer needed to be careful in assigning any functions important to safety to the computer. This was because the process of safety justification of software was not clear. Direct safety functions were implemented by traditional hard-wired indicators, alarms and trip equipment.

The UK developed the Advanced Gas Reactor (AGR). This design has temperature measurements of the coolant gas of each fuel channel. Complex functions control the temperatures using the control rods, for which computer methods were very appropriate. The UK successfully developed fault-tolerant control systems for these reactors in the early 1970's. The later systems have devoted, distributed controllers for each function. Dual redundancy and fast changeover is used with complex scheduled algorithms, in various control languages developed specifically for nuclear applications. The computer systems used were often based on systems used for process plant, but the special concerns of nuclear plants required differences. Example are in the complexity of the control algorithms and the sizes of the on-line databases which were handled. Standard products for the process industry were often found not to have the necessary capacity or functionality.

NUCLEAR REACTOR PROTECTION AND SAFETY

Reactor protection requires that fault conditions must be detected to prevent or reduce any release of activity. The basic function is to detect that a plant signal (such as the reactor neutron flux or the coolant temperature) is beyond a threshold. This generates a vote for a trip in a three- or four-channel voting system. If a fault is detected, reactor trip by dropping control rods and mitigation actions (such as starting pumps and operating valves) must be initiated. The protection functions are not usually very complex, but there are many of them. Some can be done more effectively if calculations - for example of the linear heat rating of the fuel - are done on a continuous basis. Some depend on the plant condition or power level, which introduces decision logic. The mitigation actions depend on the fault, detected from which signals have left acceptable limits. As a guide, about 80 conventional logic diagrams can represent the input conditioning and actuation logic needed for Pressurised Water Reactor (PWR) protection.

Conventional equipment involves very many cubicles of equipment for these functions. The development of computers made the possibility of a computer-based system for reactor protection attractive. Work started in USA, France and Canada on various core protection calculators and on more extensive protection system designs in about 1975. These were some of the earliest applications of computers where safety was a major concern.

In response to this, the IEC started work in about 1980 on a standard on the software for reactor safety applications. This was published as IEC880 (2) in 1986. It defines the best software engineering practice of the early '80s, and still provides a very important reference point for nuclear plants. It is not outdated, although a supplement is being written. When it was published, no other document defined requirements for process computers which have a safety role. Only the aviation industry had any technical criteria, although work on software quality assurance was being done at the time.

The recent Sizewell B PWR plant makes use of computers more extensively than ever before. The most important was the complete reactor protection function for all postulated faults of the station design. This computer-based system is therefore classed as part of the safety system. The information system has greater coverage and very greatly improved display and log facilities (Boettcher and Hickling (3)) compared to past plants. The computerised closed loop control functions are less complex than those for AGR, but have an equal safety-related role. Some of the control loop plant actuation interfaces, in particular the turbine governor and the control rod actuation system, are driven by computer equipment. In addition, almost all controls in the control room for start/stop functions are computerised, using multiplexed cables to the control room and plant.

The demonstration of the integrity of these systems to the UK safety authorities (the NII) was very important. NNC provided review and expert help in this (Betts and Welbourne (4)). The basic activity was obtaining clear evidence and high confidence that the defined safety functions are achieved completely, without exception and without any non-defined functions. The process of obtaining regulatory acceptance is covered well in the literature (ISBN 1 87634 24 5 (5)) and not discussed here. Many lessons were learnt from the process. An important work item for the IEC which has arisen is a report on the application of IEC880. This report will give interpretations of the requirements and suggest some revisions.

CLASSIFICATION OF IMPORTANCE TO SAFETY

Where safety is involved, industries develop methods of assigning functions of different importance to safety to different classes. This makes certain that all equipment important to safety is identified. It ensures suitable technical standards for design and development, simplifies quality and operational management and allows concentration of attention where safety is important. It allows methods to be followed which will give the necessary evidence for assurance of integrity to the safety authorities.

The nuclear industry has a deterministic approach to safety classes. It again provided one of the earliest systematic approaches to safety importance, and how to consider the problem of integrity of systems which prevent death or injury to people. In nuclear power, if a system forms a primary means of preventing or controlling an activity release, it is part of the safety system and must meet the highest practicable standards. But there are other systems which support safety, or whose correct functions are assumed in the theoretical safety analyses. These are termed 'safety-related' by the International Atomic Energy Agency (IAEA), as against the 'safety system'. These two classes of system together form the 'systems important to safety'.

The nuclear industry classification systems vary for each country, but the USA classification method is basic. The USA process assigns all electrical and I&C systems which form a primary means of preventing or controlling a postulated release of significant activity to the safety system at Class 1E. All other such systems are assigned to a Non Nuclear Safety Class, even if in some cases they prevent or mitigate small releases. IEEE Standards are used for all electrical and computer systems assigned to Class 1E, and to software. The US system has weaknesses, covered by specific regulations. Other countries therefore usually identify safety-related systems as well. These are needed to support safety, but do not provide the primary role in prevention or mitigation of releases.

Clearly, care must be taken to ensure satisfactory demonstration of fitness for purpose and reliability of any system. Safety systems require the highest standard. Some relaxation is allowed for the safety-related systems. To make this systematic, an important standard - IEC1226 (6) - was written. This standard sets out the criteria for identifying Category A, B and C functions, systems and equipment. In effect, automatic and manual safety functions are assigned to Category A, with safety-related systems in Category B and C. The standard IEC1226 drew from UK concepts developed for the later AGR plants and Sizewell B. The criteria are based on consideration of the reactor system faults which could cause release of radioactive material. The essential requirements for ensuring satisfactory functionality, reliability, performance, environmental durability and quality assurance are given.

It is important to define and understand the terms clearly. They are internationally agreed in nuclear power, but other process industries use the terms differently, and 'safety-related' means just that - the system is related in some way to safety, but without differentiation of how important to safety it is. Some industries use the term 'safety-critical' for the system class which may involve a risk of death.

IEC1508 (7) for the process industry defines a systematic approach for identification of the integrity needed for a protection or control system. The frequency of each hazard due to a plant malfunction must be estimated. The effects of the hazard must be considered. The effects may be possible deaths or injury. The frequency of each resulting risk is then considered. The IEC1508 approach then assigns four risk classes, depending on both the severity of each hazard and its assessed frequency. A protection system can then be defined, with a requirement that the risk is reduced to some tolerable low level by its action. This process gives a requirements for the protection system in terms of its probability of failure on demand (pfd). According to the pfd and risk class, a Safety Integrity Level (SIL) of the protection system is determined from SIL1 to SIL4 (the highest class). The SIL is then considered in terms of the system design and technical characteristics and the management measures needed to give assurance of performance to that integrity and reliability level.

IEC1508 will form an essential reference for all process systems, in all industries. The standard expects each industry to develop its own sector-specific standard, to comply with the requirements. Generically, SIL1 is broadly equivalent to normal commercial equipment with SIL4 as the highest grade of integrity. The SIL combines the failure probability due to random failures and due to systematic faults. Systematic faults can cause failure of several redundant or similar systems, as Common Cause Failure (CCF). This applies equally to conventional electronic and to programmable systems. Methods of controlling systematic fault rates are given in the standard. At a specific SIL, an electronic system requires equal attention to disciplined and controlled design and implementation as would software at the same SIL.

It is possible, in principle, to use a low SIL for a high consequence but infrequent hazard, provided the risk assessed from that hazard is sufficiently low. This design approach works provided few hazards are considered, but many hazards would need several protection systems, possibly at different SIL figures. The joint use of many protection systems is undesirable, and so in practice protection needs the highest SIL, determined from the most frequent fault considered and the worst hazard, together. In practice a classification similar to the deterministic approach of nuclear power is the result.

SYSTEM RELIABILITY

How are these classes and standards used in software with safety importance on nuclear plants? The answer is developing as the understanding of software reliability and the methods of determining a figure for reliability develop. Probabilistic Risk Assessment (PRA) methods were pioneered by the nuclear industry. PRA methods require a reliability figure for a computer-based system and its software. If a computer is used for reactor protection, what reliability figure can be used for its software? It is clearly of vital importance, both of itself and due to the public perception that software systems are not reliable. First, the requirements must be discussed.

Many national nuclear safety regulators require a PRA for the plant, typically with a requirement to show that the summed frequency of all releases is less than about one in 10^6 years. This in turn means that the reactor protection system must act with sufficient reliability to meet this figure. In round figures, since some frequent faults such as loss of feedwater can happen up to ten times per year, protection must be provided with a failure probability better than 10^{-7}. UK and other national figures are naturally more carefully expressed, but a very demanding failure probability is required. The process industry is now finding targets of safety expressed in terms of the frequency of risk to the public or to life. This makes the assessment of software system reliability very important.

DIVERSITY

It has been shown that even systems made to the highest practicable standards and with redundancy have a limit of reliability. This is due to CCF. Reliability cannot be justified to have a figure better than about 10^{-4} to 10^{-5} probability of failure on demand (pfd). The limit is given in IEC1508 (7), Part 1, 7.6.4.10. This is caused by factors of human error. These errors appear in design and operation, system requirements, earthquake tolerance, degree of fire separation, manufacturing, QA and the like.

Clearly, therefore, reliability figures of 10^{-7} pfd need two different methods of protection. Different means diverse - the differences can be in the function or in the technology used, or both. Each action should have redundancy for greater reliability. If the methods are sufficiently diverse (that is, different), their joint pfd figure is the product of the two pfd figures. Otherwise their joint pfd figure is less good, and is assessed by methods such as beta-factor weights or cut-off figures to judge CCF limits.

For satisfactory independence and diversity of two systems, IEC1508 requires functional diversity and diverse technologies, with other features of physical independence ((7), Part 1, 7.6.4.7). Only then may the reliability numbers estimated for two systems be treated as independent.

As an example of functional diversity, two differing means of shutdown of a PWR can be provided. These could be control rods, and injection of borated water to the coolant as two methods of reactivity reduction. Two methods of heat removal can similarly be provided, such as steam driven and electric emergency feedwater pumps. These would have reduced functional diversity if both pump systems feed the same boilers. As examples of diversity of technology, two protection systems can be provided. One can be a solid state, fail-safe logic design and the other a computer design.

IEC1508 says that, however diverse the technology, limits on common cause failure rates are imposed by low probability events. These include aircraft crash and earthquakes, unless special precautions are taken ((7), Part 1, 7.6.4.7). Theoretically, independence is prejudiced even if the computer and the alternative protection both use any solid state or integrated circuit components, even of different types. This makes high figures of reliability essentially impossible to achieve, if literally applied. Special physical protection, seismic testing, separation by fire barriers and independent air conditioning systems and supplies are needed, to gain system independence.

The differences in technology between different computer types can be made as great as the differences of component types. Differences in computer approach should clearly be included as well, including different micro-chips, different input and output equipment, different communications methods, different algorithms and different software engineering approaches. If the nuclear regulators in a country allow this degree of difference to give independence, two computer systems could then provide protection. The extent of these differences is clearly a subject for further R&D.

SOFTWARE TECHNOLOGY - GENERAL

The earliest approach to software was often to write code, test it, install it and then fix the bugs, at great cost. This applied to the nuclear industry, and it appears that the process industry had equal or even worse experience of this approach. Technology advanced, and more structured methods with proper documentation developed.

As an example, NNC developed a simple method of defining closed loop and sequence control software for the AGRs commissioned in the late '70s. It was developed further for Torness AGR. This required the control engineer to express the requirements first in a traditional form, and then in a pseudo-code form. This was then coded by hand by the programmer, using direct code, macros and subroutines. A software test harness was used to drive the software in a single pass mode and record the output response to sets of input data. The test data and response were defined by the control engineer. The programmer was required to produce code which met these tests, operating in the test harness. This caused a two-way interchange with the control engineer until code, requirements and tests were consistent. Handover to the site testing team required correct output from the test harness. The site testing team made formal reports of any shortcomings of the software with respect to the original traditional form and the plant completion tests. Again this resulted in a two-way exchange with the designers until design and performance were consistent.

Three lessons were learnt from this on high integrity software production, although their importance was not fully realised at the time. These lessons are:

- the requirements must be formally and fully expressed,
- the requirements must be shown to be achieved, and
- the testing must have independence from the designers and programmers.

An analysis of the performance of the control and sequence functions was made much later for one plant. This showed that no modification had been made for software errors (4) from the time of handover for operational use. There had been many system modifications due to changing control requirements, but not for software errors.

SOFTWARE TECHNOLOGY - SAFETY SYSTEMS

In France, the 1300 MW series of PWR plants provide all reactor protection using a distributed micro-computer system known as SPIN. There are 20 such plants reported with 100 plant-years of successful operation ((8) Aappendix III). The software of SPIN was developed basically in accordance with the recommendations of IEC880, as about 40,000 lines in 6800 assembler. An interesting feature of the system design is that, to supplement the reliability claimed for the SPIN system, an additional separated system supports the safety system. This system is not classified as part of the safety system and operates only for the more frequently expected faults of the design basis. It is also computer-based, and implemented in a process control range of dual channel modules with automatic failure detection features. The SPIN system is understood to be claimed at about 10^{-4} pfd. In addition, about 10^{-2} pfd is claimed for the support system and the two systems are claimed as independent. Both use computer technology but in very different ways.

In Canada, the CANDU reactor design requires two independent and different safety systems, which have differing functional methods of shutting down the reactor. The most recent Darlington plant (about 40 miles from Toronto) has two independent computer-based systems. One has micros and the other minis, using different software methods and languages for these functions. The design took account of CCF potential arising from common algorithms for threshold detection or voting in the two requirements. They are understood to be claimed as independent at about 10^{-4} pfd each.

When the implementation was at an advanced stage, the Canadian safety regulators decided to apply IEC880 requirements. They also questioned the accuracy, consistency and completeness of the implementation and required very extensive extra work to be done to provide evidence of the integrity claimed. This included expressing the requirements using a formal methods language (using a strict formal logic notation), and analysis of the code for both systems to show failure propagation paths and identify critical points. The system was operated against a random trip trajectory generator, to demonstrate about 10,000 successful trip actions for confidence in reliability. Very great effort was expended to provide this evidence of accuracy, completeness, correctness and reliability. This has resulted in a very closely defined set of standards, agreed between the three parties of designer, utility and regulator. This covers implementation of software for safety or safety-related functions ((8) Appendix III). These standards are applied to the CANDU constructed in Korea.

In the USA, various systems were installed for core protection, and included retrofit systems to upgrade outdated solid state protection equipment. Some safety display equipment was installed for post-fault monitoring. The earlier systems are understood to have been implemented in accordance with IEC880, and a very high software reliability was achieved. The USA regulators are understood now to require compliance to IEEE 7-4.3.2-1993 (9). Compliance with other IEEE standards on V&V and documentation is required. Some form of independent verification and validation are needed. Their position is still developing.

The Sizewell B application of computers to protection in UK is described in (5). The UK regulators had learnt from the Canadian experience and from UK military applications of computers, and required comprehensive demonstrations of integrity. The process required document and code review, independent assessment and response, code analysis, and demonstration that target code matched source code. Also tracing between requirements and implementation, and random trajectory testing using a dynamic test harness was needed. This involved considerable cost, quoted in (5) as 250 man years of effort for about 100,000 lines of code.

CLASSIFICATION APPLIED TO COMPUTER SYSTEMS

A closed loop control system and an information and display computer system would be classed as Category B and C respectively under IEC1226. A SIL2 or lower system under IEC1508 would normally meet the reliability requirements, but might not meet the nuclear power requirements at Category B. Documentation could be needed to a higher standard for Category B. Any

Commercial Off-The-Shelf (COTS) software used will need to be justified to the regulators. An assessment of the risk of Common Cause Failure (CCF) between different control loops using the same modules may be needed. To meet this problem, the IEC is developing a supplement to IEC880 to widen its application to cover Category A and B systems. This supplement includes sections on CCF, formal methods, software tools, use of existing software and application of IEC880 at Category A and B, together with informative appendices.

The CCF section of the supplement to IEC880 defines requirements for identification of sources and effects of CCF. Means to prevent CCF should be included, with an estimate of failure probability. This is important for redundant voting systems for protection, and for different Category B controllers using the same software modules. The formal methods section identifies the necessary characteristics of such methods, if they are to be used. The section on tools and their role identifies tools for transformation, verification and validation, services and configuration management. It recommends documentation on the role and qualification of the tools for use. It covers the generation of the signal configuration information and discusses compilation and testing tools. It requires software tools at the standards of the application category if the tool output cannot be verified and validated off-line. The section on use of existing software defines the process of information gathering and assessment. This is followed by an evaluation process to judge the useability of the software element at Category A or at Category B. The application of IEC880 at Category B is described and some technical relaxation is possible from Category A. Generally documentation is required to the same standard with similar verification and validation.

APPLICATIONS

On many older process plants, the original plant instrumentation system and information computer need replacement. The replacement system can take advantage of information available from multiplexed plant data. Computer hardware is more reliable, and is smaller than conventional hardware for the same functions. This simplifies finding a place to put refit hardware. Multiplexing allows savings by use for several purposes of a single instrument. Multiplexed cables to control switches and to switchgear reduce cables to a minimum. The computer equipment can also be distributed physically around the plant. Distribution avoids using space near the control room, which is often already full of equipment, and allows installation in parallel with use of the old equipment.

Computers therefore have great attractions for refit of process plant. An important example is the Russian design of pressurised water reactor, known as the 'VVER', where the existing cable races are very full. The VVER designs used many instruments each with one use, due to poor performance of the original instruments.

Computer protection allows calculated trips to improve the protection and to reduce excessive margins, which were needed where a hardware based system used straight-line approximations to calculations. The advantages of smaller, more reliable equipment, with multiplexed information and distributed in the plant also exist.

Some of the applications to VVER will be at IEC1226 Category A or B. For example, closed loop control is at Category B and control of safety plant and safety parameter display is at Category A. Reactor protection and any other Category A application using computers require careful consideration of the cost of demonstrating integrity. Demonstration at Category B will be less demanding. Demonstration of integrity will be difficult if COTS software is used, and this is essential for Category B.

Utilities who operate VVER designs recognise the advantages of computers for protection, and understand the need for diverse protection. Their reliability targets for preventing any release are similar to those of Western nations. The regulatory authorities are often still developing their attitudes to accepting safety system software, but have also understood the need for clear evidence of integrity. Some nations have adopted an approach based on the USA process of acceptance of safety-critical software. This requires an Independent Verification and Validation (IV&V), in which an independent organisation is contracted to review the software design, implementation, verification and validation. Additional testing can be required, and may be undertaken by the IV&V contractor. Code analysis for accuracy and completeness may be used to give confidence in the integrity of samples of code, or of all code. This depends on the judgement of the IV&V contractor. This simplifies the process compared to that which has been used in UK.

There should therefore be some caution in recommending a computer-based system for protection, due to the uncertainty of cost in obtaining regulatory acceptance. If a plant can exploit the previous qualification of suitable software, computers will have an advantage. If a second computer-based system is suggested, again caution is needed. The reliability claim must be made on the basis that the two systems are truly independent and that the use of common technology is acceptable, as outlined earlier.

CONCLUSIONS

The use of computers on nuclear and process plants has grown steadily in all nations, and the need for R&D into some central problems is considerable. Some of the main problems of safety-critical software have a close link with system design, emphasised in this paper. These involve the reliability of protection, the use of redundancy and the possibility of CCF. The production of evidence for the certainty and integrity of the implementation of requirements is another aspect. An important problem is the definition of requirements. Operational handover of very high integrity software systems involves implementation and commissioning to very high standards. After this stage, informal reports are that roughly equal numbers of defects are found which originate from requirements as from implementation. This needs more careful and disciplined investigation and reporting.

The successful implementation of a safety-critical process plant function, a reactor protection system or a safety plant control function by computer will depend on the requirements specification. It should be shown that they are complete, consistent and not ambiguous. Formal methods of expressing requirements allows tools to be used to show this. So this process should reduce the number of errors in requirements. Few applications of this method have yet been done outside the defence industry. They are proven, although costly. Simpler methods are becoming available. The process and nuclear industries need trial application of the methods, some of which have been used successfully in avionics.

Other areas of importance, not discussed in detail, are the Human-Machine Interface (HMI). Up to 30,000 signals need display on a typical modern nuclear plant. Alarm flooding of displays at plant trips, and the design of clear information displays are both areas of R&D with equal application to many types of process plants as to nuclear. Integration of plant operating instructions with on-screen control is possible, and NNC have produced demonstration software to show the principles (Humble and Welbourne (10)). Improved human factors and task analysis input to VDU displays is still needed for clear and simple-to-use displays of the very large amount of data.

An important computer application in the process industry is soft, on-screen control by touch or cursor methods. Selection of a plant item for display shows a control target on the screen. The operator can select open and close, or equivalent actions, or select sequences for action by the computer system on the target. Selection may be by mouse, roller ball or by touch. Plant control panels are greatly simplified, and many cables are saved. Control stations can be distributed and standardised. Nuclear plants in France and in the Czech republic are including these facilities now. But many problems of demonstration of the integrity of the selection process can be expected. The safety regulators will want evidence that the process cannot ever cause the wrong item to be selected. The use of a proprietary system for soft control of a safety function on a nuclear plant would involve close analysis for the software path from screen target to control actuator.

The UK is unlikely to start a new nuclear power plant for some years. A new plant will involve extensive computers, with high reliability and integrity requirements. These require skills in the latest computer and system engineering methods. NNC is actively involved in project management and design for nuclear plants, especially for VVER and RBMK plants (the pressure tube, graphite moderated reactor plant type of the Chernobyl accident). Computer system design and refit is important for these plants. These projects and experience of process plants allow the nuclear industry to develop its expertise. The industry will require those skills to implement computer systems to meet the high reliability targets of nuclear plant.

The application of the methods of IEC1508 gives a systematic method of approaching the problem of system and software reliability. When it is fully agreed, it will allow a supplier of systems and software to state that a product meets the requirements for a specific SIL. It will therefore be possible to use a known product to meet a required level of reliability with confidence, *even if it includes software. This will clearly be of considerable benefit to the designers of systems,* the process industry, and the industries which serve the process industry. Records of their performance must be available to the safety authorities. The records will be a sales advantage, and, it is hoped, they will be available to the public. The process industry can therefore give a lead in producing high integrity computer systems.

REFERENCES

1 Application of digital computers to nuclear reactor instrumentation and control, IEC643:1979.

2 Software for computers in the safety systems of nuclear power station, IEC880:1986.

3 Boettcher, D. B. and Hickling, E. M., Man and machine will work in harmony in the main control room at Sizewell B. Nuclear Engineering International, September 1993.

4 Betts, A.E. and Welbourne, D., Software safety assessment and the Sizewell B applications. IEE Conference - Electrical and Control Aspects of the Sizewell B PWR, Churchill College, Cambridge, 14-16 September 1992.

5 *Proceedings of a Forum on Safety Related Systems in Nuclear Applications* - 28 October 1992. The Royal Academy of Engineering. ISBN 1 871634 24 5. Summarised as - Sizewell B reactor protection reliability: Nuclear Electric presents its case - Nuclear Engineering International, March 1993.

6 Nuclear power plants - Instrumentation and control systems important to safety - Classification, IEC1226:1993.

7 Functional safety: Safety related systems, Draft International Standard IEC1508 (6 parts), provided by BSI as 95/208053-59, Sept 95, and by IEC as documents 65A/***/CDV or /CD, with *** as 179 to 185.

8 Verification and validation of software related to nuclear power plant control and instrumentation, completed and to be published in IAEA Report Series, Vienna, 1996.

9 IEEE Standard criteria for digital computers in safety systems of nuclear power generating stations, IEEE Standard 7-4.3.2-1993.

10 Humble, P.J. and Welbourne, D., VDU display in accidents - *Interact*, IAEA Specialists Meeting, Springfields UK, 15-19 July 1996, to be published.