INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA

NUCLEAR SAFETY REVIEW 1995

TECHNICAL CO-OPERATION
NUCLEAR POWER
NUCLEAR FUEL CYCLE
HUMAN HEALTH
INDUSTRY & HYDROLOGY
PHYSICS & CHEMISTRY
RADIATION SAFETY
NUCLEAR SAFETY
SAFEGUARDS

PART D OF THE
IAEA YEARBOOK
1995

NUCLEAR SAFETY REVIEW

Contributors

IAEA Division of Nuclear Safety

F.N. Flakus
A. Gürpinar
J. Hashmi
K. Hide
A. Karbassioun
(technical co-ordinator)
L. Lederman
J. Pachner
R. Seiberling
P. Stegnar
B. Thomas
G.A.M. Webb
Wanli Zhong

External Contributors

R. Clarke, United Kingdom
P.J. Courtois, Belgium
J. Heltemes, USA
L. Reynes, France
M. Sjöberg, Sweden
R.L. Tapping, Canada

Software Safety Issues in Nuclear Applications and Installations

P.J. Courtois
AV NUCLEAR
Brussels, Belgium

1. Introduction

The use of software in situations where human safety is at risk, is growing fast. It has indeed been recognized by different industrial sectors that some technical and economical properties of the software technology can contribute to the improvement of the control and safety function in critical applications. Software implementations allow more intelligent on-line monitoring and diagnostic aids, are more easily tuned and adapted, do not wear out with time, are not affected by the environment, are cheaper than their hardware equivalent, and more accurate and stable.

At the same time however, it has also been recognized that the design and the validation of predictably dependable software for safety -critical or -related applications raise difficulties that are specific and different from those raised by the design of equivalent analogue circuits.

Software implementations tend to have a richer functionality, and thereby to be more complex and more prone to design errors than the analogue implementations they replace. Besides, software implementations are discrete models of the real world. Thereby, they are more sensitive (i.e. less tolerant) to "small" errors; they are also more difficult to test, because continuity arguments are not valid and interpolation is not feasible.

These problems are now receiving much attention from scientists and experts in computer science and software engineering. However, these disciplines have not yet succeeded to agree upon a definition of a set of minimal skills required from programmers, nor upon the techniques of design and validation that could be enforced to produce predictably dependable software.

2. The Present Situation in NPP's

Computers have been successfully used in NPP's for many years, but were usually backed-up by hard-wired systems when safety was at stake. It was only recently with the adoption of fully computerized logic into reactor shutdown systems and other safety-critical or -related systems, that the problem of software integrity clearly arose, and - as will be illustrated and explained below - especially from a regulatory standpoint.

Among the leading countries in the development of fully computerized nuclear control and protection systems are France, U.K., and Canada. Some of their endeavours have been successfull, while others, unfortunately, have been notoriously marred by costly mistakes and failures. Some of these good and bad fortunes are briefly evoked by the examples below. Similar situations, however, did and will arise in other countries as new NPP functionalities are being implemented in software, and old analogue equipments are being replaced by digital systems (backfittings).

● In France, the SPIN 1300 micro-processor based system is one of the most widespread computerized protection system. Since the first 1300 MW PWR connection to the network in 1984, it can refer to a field experience of about 100 reactor-years of operation. The SPIN 1300 software consists of 40.000 assembler instructions, and 1100 defects had been detected and corrected during the development phases [8]. But only three minor bugs are reported [7] to have been found during that period, none of them causing any command masking.

Strenghtened by this 1300MW experience, the use of micro-processors was generalized in the new N4 1400 MW PWR design. But the sophisticated P20 hardware and software originally intended for the original I & C Control logic of the N4 design, had to be abandoned. It was reported that it is not the hardware that posed problems. But faced with major difficulties in perfecting the product, and the huge software complexity of the system, there was no certainty that the programs could be qualified to stringent dependability requirements. This forced to switch the I&C logic during the development to an existing computerized control system not specifically designed for nuclear use, and at the request of the safety authority, to move safety support functions into the SPIN environment.

This new SPIN N4 system which incorporates these functions consists of about 200.000 instructions. In response to an earlier requirement from the safety authority that this system be sufficiently protected against common mode software failures, it was proposed to install hard-wired backups for systems involved in accident sequences considered as most probable (loss of secondary coolant). Late in 1993, this was not felt sufficient, and the authority asked to consider which additional computerized protection systems should be backed up by hard-wired connections to diversify protection against further low probability or hypothetical accident sequences that can lead to fuel damage or core melt [7].

- Sizewell B, the latest nuclear power station to be built in UK, is about to enter service. There are two automatic protection systems at Sizewell B, based on diverse technologies. The primary protection system (PPS) is is a microprocessor based system while the Secondary Protection System (SPS) is built of conventional analogue trip units and laddic magnetic logic elements, without computers and without even simple software. The SPS should provide a back up to the PPS for reactor trip after all faults; it also should back up the PPs to start safety features automatically after 'frequent' faults - faults of frequency higher than 10^{-3}/yr. For infrequent faults (< 10^{-3}/yr), the SPS does not automatically start the safety features, although it is supposed to trip the reactor [9]. The PPS incorporates sophisticated protection monitoring, provides diagnostic aids, can accomodate design modifications during the design and during operations, and provides also automatic routine testing and calibration.

These desirable features, among others, explain the complexity of the system and its size (about 100.000 lines of unique code). Huge efforts have been spent on the analysis and the testing of this code (more than 300 man-years). But, despite the SPS backup and these verification efforts, the complexity of the PPS software raised serious concerns from experts and computer scientists [2]. And mid 1993, the safety authority reached the view that, while they considered the software to be of a high quality, they could not be fully confident, from the demonstration provided so far, that the original integrity target (10^{-4} pfd) for the system had been achieved; they were confident, however, that the shortfall was not unacceptable, because the plant safety case could accomodate, without significant detriment, a lower integrity for the PPS (10^{-3} pfd).

- In Canada, the verification of the emergency shutdown software for the Darlington nuclear power plant is perhaps one of the most ambitious software verification by formal methods that has ever been attempted for an industrial safety critical application. The plant has two independent dedicated shutdown systems. Both are implemented in software and relatively small (in the order of ten thousands lines). Software diversity is achieved at the functional level: one system operates by rod dropping, the other by moderator poisoning.

State of the art formal methods, making use of mathematical function tables, were applied to convince the authority that the software was of acceptable quality and in accordance with specifications. This verification effort took over two years and, alone, cost between $2 and 4 million Canadian. At some point, up to thirty people were working on different aspects of the verification. It resulted in about one hundred modifications to the software, all relatively minor. In 1990, the authority issued a license for full power. But it also stated that the software was not designed so that it could be easily maintained; it was difficult to determine what the impact of even a minor change might be. Therefore changes in the software might require extensive review, and this was not felt practical for long-term used. An extensive redesign was therefore recommended for the medium to longer term [3]. It was also felt that the software had not been designed with formal methods in mind, and that, in the future, designers should keep in mind what verification tasks need to be performed, and develop the software accordingly.

An attempt at drawing some lessons from these experiences is made in section 4.

3. Prospects

Despite the problems evoked in the previous section, many operators and designers seem determined not to go back on their choice of computerized I&C [7], as if the question of whether it is safe or not to allow the safety systems of NPP's to be controlled by computers had already been answered. In few cases however, Tihangel in Belgium for instance, the decision has been taken to use classical technologies (e.g. failsafe magneto-static elements) to replace old I&C systems. Preponderant reasons that are often put forward to justify this conservative attitud are the uncertainties and difficulties associated with the licensing of safety critical software, and the lack of preparedness and expertise of nuclear experts and technicians in the new information technologies. This lack of expertise among operators and regulators also explains the unrational arguments on which are sometimes based the attitudes and the decisions of those who can influence the technological choices.

Nevertherless, at Temelin, in the Czech Republic, it is planned to replace the original plant I&C system designed by Soviet and Czechoslovak companies in the eighties by a computer based system for reactor protection and control, post-accident monitoring, in-core instrumentation, and plant control functions. The software will thus be of a complexity that is comparable to that of Sizewell B. An IAEA technical co-operation expert mission was set up by the IAEA in 1994 to assist the Czech regulatory authorities with the licensing of this I&C system.

The German Reactor Safety Commission (RSK), and the French Advisory Group "Groupe Permanent Chargé des Réacteurs Nucléaires (GPR)" have adopted common recommendations for the safety of future PWR plants in the framework of the advanced reactor development joint project, called European Pressurized water reactor (EPR) project. These recommendations stipulate that emphasis should be placed on the use of computer techniques for diagnosis systems for operator support. So far, nothing has been said however on the qualification of software, leaving the initiative to the designer for providing specific proposals concerning the qualification of such computerized systems and of their software [10].

Interest groups have been raised to discuss and share common experience with the aim of finding solutions to the issues raised by the licensing of nuclear safety critical software. For example, in Canada, the National Research Council has organised a Software Reliability Interest Group (SRIP), involving military and governement departments directly concerned with purchase or approval of safety related software. Internationally the IAEA has created a technical committee made up of a range of nuclear power users and regulators to focus on the problem and hopefully to produce guidelines [1]. The OECD has also set up a working party.

Regular but unofficial contacts take place between the nuclear power regulatory authorities of U.S, Canada, France, U.K. and Japan on issues involving safety of advanced digital instrumentation and control systems [4],[6].

The IAEA has been one of the more active international bodies in the field, its activities culminating in 1994 with the publication of a technical report on Software important to safety in Nuclear Power Plants [1].

4. A Common Root Cause

It does not take a long analysis to reach the conclusion that the origin of the software system costs, delays and failures discussed in section 2 can all be traced back to a common set of causes.

It is universally accepted that for software important to safety, there is a need for thorough independent verifications and validations (V&V) before it is placed into service. However, in each case mentioned above, a trustworthy independent review of the end product turned out to be either impossible, or very hard at the least. The software could simply not be approved, or could only be approved after extremely costly re-documenting or re-design, causing severe penalties in terms of delays and unprofitable equipment investments.

Although these systems were not proven to be unable to satisfy their safety requirements, it was very hard or even impossible to obtain from safety authorities sufficient confidence in these systems' ability to satisfy their requirements. In many cases, the reality was that the regulatory confidence in the software had to be obtained by assessment of an already finished product when, in fact, this is usually unfeasible. It is indeed impossible to fully test software systems of that size. Besides, software important to safety is in the nuclear industry software that most work under "first use". It is not practical to observe its performances under real accident conditions before it is placed in service. It is also software that most often is dedicated to a single installation, and runs in very few copies. Its reliability cannot be inferred from past usage that has stood the test of time.

Thus, the "black-box" approach alone, is technically unsufficient to assess software and gain confidence in it. Not only the product, but the design process itself must be monitored and assessed. After all, software is an intellectual construction, and as such (i.e. leaving aside the hardware on which it runs), is entirely determined by its production process.

The necessity of this shift of emphasis from software product to process assessment is well discussed in [11]. Nuclear safety authorities, more used to product performances than to design approval, and concerned with keeping their independence of judgement, do not always sufficiently perceive this necessity.

The aspects of the software production process that have a major impact on the qualities of the end product are:

- The competence and experience of system designers and programmers;
- The design, programming and validation disciplines which are enforced;
- The design, programming and validation tools used;
- The documentation on design, software, computers and tools made currently available

during the process;

Good practices on these aspects (staff, disciplines, documentation and tools) are all essential to contribute to the absence of software defects in the end product, and need monitoring. But it is our experience that in the validation of software and the process of design assessment emphasized above, documentation and tools play a special role.

5. Reviewability

Independent V&V of safety critical software implies that experts who did not participate in the design must be able to understand the programs. To "understand a program" does not mean simply to understand "each line of the program, and what each instruction does and why the programmer thought it was necessary" [12]. It means an ability to convince oneself (and others) with good reasons that the programs will work, in every detail, as required by the specifications.

Because of the complexity of real software, this kind of understanding is not achievable without the aid of a detailed but well structured and clear documentation of the programs.

This documentation is the help from program's designers that reviewers should expect. It must make possible to trace in the code every requirement and design decision. This implies that, *ab initio*, the application and software requirements, the design and programming specifications, and the code must be carefully structured and documented for review. Code reviewability must be a design requirement. Writing reviewable documentation must be part of the design itself.

More attention must be paid to those requirements and attributes that are necessary to achieve software important to safety of a quality that facilitates reviews and allows reviewers to be confident of their conclusions. These requirements and attributes pertain to the different stages of the software development process (system requirements, software requirements, program design), as well as to the documentation and test reporting which must be auditable.

The Darlington software is an example of an attempt at producing reviewable code documentation (see a.o.[13]). Research work is planned in the last phase of the European CEC ESPRIT strategic programme on information technologies on methods and models to design computer based systems when validation is a primary requirement [14]. But, in general, it is fair to say that reviewability is a design requirement that has been very much neglected in the nuclear I&C industry, in Europe in particular, and by industry as well as by the regulators.

6. Tools

It is not desirable that every new software system be developped from scratch and manually from the application level down to the bit level. If one assume that, on the average, programmers' abilities do not change much with time, the quality of software produced in this way is unlikely to improve with time.

The quality of tools like compilers and code generators has the potentiality of improving usage as defects are found and corrected. If they are properly validated, tools which produce code mechanically allow reviewers to concentrate on the application part and on programs written in high level programming or application-dependent languages. The documentation needed for reviewability is reduced accordingly, being essentially restricted to the application level. Of course, the validation of a tool, by any means, is not easier than the validation of any program. But it has the advantage to capitalize quality from project to project. Again, too little effort is being devoted to the validation of tools.

7. Summary

The problems raised by the recent developments of software fullfilling safety functions in nuclear power plants appear to have a common cause: the difficulty of convincing independent reviewers of the ability of the software to satisfy its requirements. These problems would have been eased if the software had been conceived and designed, right from the outset, according to requirements and attributes that facilitate reviewability. Documentation and code generating tools that are properly validated are essential means to achieve this objective.

Interactions and harmonization among countries on those issues is of utmost importance for the future of nuclear industry, as software retro-fittings and new systems are creeping in. A framework of requirements that assure the reviewability is essential to licensing software products that must be trustworthy.

9. References

1. *Software Important to Safety in Nuclear Power Plants.* International Atomic Energy Agency, Vienna, Technical Reports Series N° 367, 1994.

2. *Proceedings of a Forum on Safety Related Systems in Nuclear Applications.* The Royal Academy of Engineering, London, October 1992.

3. *Case Study: Darlington Nuclear Generating Station.* D.Craigen, S. Gerhart, R.T. Ralston, IEEE Software, pp. 30-32, January 1994.

4. *USNRC Office of Information Resources Management. Items of Interests.* Week ending May 28, 1993

5. *Regulatory Approach on Digital Instrumentation and Control Systems for Future Advanced Nuclear Power Plants.* U.S. Nuclear Regulatory Commission. Division of

reactors Controls and Human factors, SECY-93-087. 1993

6. *Digital Computer Systems for Advanced Light Water Reactors*. U.S. Nuclear Regulatory Commission, SECY-91-292, 1991

7. *INSIDE N.R.C.* July 11 1994, pp. 5-6

8. *Qualification des Logiciels*. C. Esmenjaud, A. Parry, Présentation aux Journées SFEN Sûreté et Contrôle-Commande des Centrales Nucléaires. Retour d'experience du contrôle-commande informatisé. 22 mars 1994.

9. *State of the Art at Sizewell B.* D. Boettcher, ATOM, AEA Technology, March/April 1994, pp.34-38.

10. *GPR/RSK Proposal for a Common safety Approach for Future Pressurized water Reactors*. Adopted during the GPR/RSK meeting on May 25, 1993, Bundesamt für Strahlenschutz RSK-Geschäftsstelle, Husarenstrasse, 53117 Bonn.

11. *Viewpoint*. J.-C. Laprie, B. Littlewood, Communications of the ACM, 35, 2, 13-21.

12. *Evaluation Standards for Safety Critical Software*. Final report, Part 1. D.L. Parnas, A.J. van Schouwen, Po Kwan, Queens University, Kingston, Ontario, Canada.

13. *Assessment of Safety Critical Software in Nuclear Power Plants*. D.L. Parnas, G.J.K. Asmis, J. Madey, Nuclear Safety, 32, 2, pp. 189-198, 1991.

14. *Predictably Dependable Computing Systems*. Esprit Basic Research Project 6362-PDCS2, Commission of the European Communities, Brussels.

(end of document)