ISSN: 0974-6471, Vol. 11, No. (3) 2018, Pg. 169-178

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Study and Comparison of Integrated Circuits in Digital and Analog Form of Present Day Technology – Review

E.N. GANESH

Soe Vistas Chennai, India.

Abstract

Fifty years ago instrumentation and control (I&C) systems at nuclear power plants (NPP) were analog and relied on a mixture of mechanical, pneumatic and electric components. Today analog technology has been replaced with digital technology. Digital I&C has over the years experienced difficulties in the licensing process, which has delayed and escalated costs of both NPP and I&C projects. In the paper it is argued that some of the difficulties are connected to misunderstandings regarding differences between analog and digital I&C. These misunderstandings have led to unrealistic expectations regarding proofs that selected I&C systems can be considered acceptable. To ensure a successful licensing process it would be necessary to agree on evidence for safety that can be considered sufficient. Such evidence should be collected both from the I&C design process and from testing intermediate and final I&C solutions. By a combination of evidence from different sources it should be possible to build a safety case that can be agreed to give sufficient proofs for acceptability. The first component in building the safety case is to make use of safety principles to provide structural evidence that certain classes of design errors have been avoided. The second component is to use simulators and targeted testing to demonstrate functionality of the I&C in different plant situations.

Article History

Received: 11 July 2018
Accepted: 30 September 2018

Keywords

Analog,
Digital,
I&C functions,
Safety principles,
Verification and
Validation.

Introduction

The development of instrumentation and control (I&C) has been tremendous the last fifty years. In the 1960ies the I&C systems were analog and relied on a mixture of mechanical, pneumatic and electric components. Today the analog technology has almost entirely been replaced with digital technology. A rapid development of digital I&C started with the advent of microprocessors in the 1970ies. The first systems were restricted to simple control tasks and they were not flexible enough to be used for advanced control loops. A decade later the conventional power industry had moved to the new systems to make use of their advantages. The nuclear was very much slower in applying digital I&C systems. One reason is that not many new nuclear

CONTACT E.N.Ganesh enganesh50@gmail.com Soe Vistas Chennai, India.

Doi: http://dx.doi.org/10.13005/ojcst11.03.05

power plants (NPP) have been built after the 1980ies, which implied that digital I&C projects were restricted to modernizations. Another reason for the slowness was the need to provide convincing proofs that digital I&C systems are safe. Proposals to use digital I&C led to extensive discussions on their acceptability for safety and safety related applications. The concern was the complexity of software based systems that made complete evaluations of their functionality impossible. A common argument was that one could never be sure that digital systems would function on demand as intended and would never exhibit spurious unsafe actions.

Digital I&C have many advantages over analog I&C, but to achieve the advantages the design process as well as the licensing process should be adapted to the new technology. Today it is an accepted fact that confidence in digital I&C has to build on information both from the design process and from testing the designed product. Consequently the licensing process should build its safety case both on conjectural reasoning from the design process and on empirical evidence from testing. By using structural information on design solutions and combining it with targeted testing, it should be possible to create sufficient arguments to prove that digital I&C systems are safe enough. It is proposed in a companion paper that safety principles used in the I&C design processes can provide arguments that certain design errors have been avoided.[1]

Functions of I&C Systems

A functional structure of I&C systems at power plants was well established already fifty years ago. Functions in present I&C systems have pretty much followed the division from that time. In the discussion below I use the list of contents of the document[2], which is an early contribution of the IAEA Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI). This document also contains descriptions of I&C solutions from five countries, Canada, France, Germany, Japan and Sweden.

Design Concepts of I&C

At the start of a I&C design project there are many issues to resolve. At a general level the functions of analog and digital I&C are very similar. The first important task is to define a basic I&C design philosophy. It should be developed in close cooperation with the development of the plant design basis, where major decisions on plant characteristics and safety philosophy are made. Tasks and decisions involve establishing a preliminary safety analysis of the plant together with a classification of structures, systems and components (SSC) regarding their importance for safety.

On the lowest functional level, simple switching logic and on/off open-loop controls can be found.

For the old NPPs the I&C on this level was realized with relays. In the digital I&C systems different variations of logic circuits and processor based solutions can be found. On the next higher level there are open and closed loop controls for continuous process variables, which in the analog I&C was realized with mechanical, pneumatic, hydraulic and electrical components. On this level processor based solutions in digital I&C systems are used today.

The level of automation was much lower in the NPPs fifty years ago as compared with typical solutions today. However, in the decision on what should be automated and what should remain as manual controls, not much has changed and the paper[3] from the year 1983 is still very relevant. Process computers were used in NPPs already in the 1970ies, but mainly with the function of giving control room operators' information that was based calculations difficult to realize with analog components. The computers were at that time considered as not important for safety and no credit was taken for their functionality. Today the computational power of simple microprocessors by far exceeds the computational power of these early process computers.

Operator/Plant Communication

Operator/plant communication takes place in the main control room and via control boards located outside the main control room. This area has gone through major developments since solutions that were in use fifty years ago. One may say that the majority of the communication today uses digital systems. However, there are still arguments that at least some of the communication channels should use direct non-computerized connections.

Old control rooms were realized with meters and switches, where they today mainly use visual display units (VDU). This development has been beneficial for safety, because it is easy to combine information from different sources in a flexible way. On the other hand it is necessary to apply careful human factors engineering to ensure that operators understand and can use displays and controls.

A typical requirement is that there should be an emergency control room from which it is possible to shut down the NPP if the main control room has to be evacuated. In addition there may be arguments to include also other control facilities, such as revision planning and monitoring room and/or a technical support center. Such solutions are possible with digital I&C.

Instrumentation

In a NPP there are many specialized instruments, which will need their own considerations and interfaces to the rest of the I&C. In this category there is for example nuclear instrumentation for core monitoring, instrumentation of main components such as reactor, turbine, generator, etc. Specialized instrumentation is used also for monitoring of radiation, equipment vibrations, seismic activity, building conditions, environmental variables, etc. A common trend today is that these functions are realized with the plant wide I&C system in use.

Main Control Systems

Main control systems encompass control of all large components. Today most of these controls are automated using the plant wide digital I&C system. Selected solutions depend on the type of reactor and if the plant is designed for base load or for load following. In principle there are not large differences in functionality between the analog and digital I&C for these controls. Many new NPPs have advanced sequence controls that start and stop process systems in an orderly manner during plant startups and shut downs.

Reactor control ensures that the thermal power of the reactor follows set points that are determined by a combination of neutron flux, pressures and temperatures. Control actions depend on the reactor type, but are usually connected to control rods (PWR) or speed of main circulation pumps (BWR). For newer reactors there is often a possibility to influence the spatial power distribution in the reactor.

Turbine control in NPPs is very similar to turbine controls in conventional power plants, which eans that load demands are set either by the thermal power or generator load. In addition to these controls there are many other important controls, such as for example steam generator control, pressurizer control, volume and boron control, feed-water temperature control, condenser make-up control and generator voltage control.

Safety Systems and Safety Related Systems

I&C for safety and safety related systems are defined in the plant design basis. The requirements on these systems depend on their safety classifications and are defined through a set of postulated initiating events (PIE), that the NPP should be able to cope with.

In designing safety actuation systems there are many considerations that should be taken into account. Firstly the required redundancy is defined through the safety philosophy of the NPP. Secondly the priority of various systems should be defined and it is common to require that safety systems should have priority over other systems. Another typical requirement is that it should be possible to manually override (initiate, prevent) actuation.

Typical safety related systems are equipment that provide cooling, lubrication and electric power for main components and their safety systems. In this connection it is also important to ensure that cable routes, types, dimensions and fuses are carefully selected to avoid interdependencies through overheating, short circuits and strokes of lightning. There are also other systems that may be considered safety related, such as limitation systems, alarm systems and computer systems. Instrumentation to be used in post-accident conditions also falls in this class. The required functionality for safety related systems is not depending on analog or digital implementation.

Difference between Analog and Digital I&C

The introduction of digital technology implied a major change in thinking and design of I&C. Functionally the

change was a transfer from continuous to sampled time and from continuous to discretized signals. Today this change may be considered insignificant, but there are salient differences, which should be understood in how they influence possibilities to provide evidence that digital I&C system can be considered safe.

Time and Frequency Issues

A move from continuous to sampled time systems means that system behavior is characterized by difference equations instead of differential equations. For control systems this can be seen as a transfer from a frequency to a time domain. Analog systems are characterized by their upper limit frequency f_u, whereas the function of digital systems is determined by their sampling interval Δt. According to the sampling theorem of Shannon the upper limit frequency fu and the sampling interval Δt are related in such a way that a time continuous signal can be restored from its sampled version provided that $f_u \leq 1/2\Delta t$. For digital systems the sampling interval Δt places a limit on system behavior, because calculations for a time step should be done in less time than Δt. For analog systems there are no similar limits because components are working in parallel. Analog systems are generally well behaved as long computations are limited to the dynamic range of the components and the upper limit frequency of signals is less than f_u. For analog systems it is therefore possible to use continuity properties when pondering system behavior in different points of their state space. If a system exhibits intended behavior in a situation A and in a related situation B, it can be argued that it will show intended behavior also when $C=\alpha A+(1-\alpha)B$, where $0<\alpha<1$.

Continuous Versus Discretized

A move from continuous to sampled time implies that the value space of the signal becomes quantified into discrete values. Important in this connection is how many bits are used in the quantification. Typical analog signals have an accuracy of about three digits, which means that ten bits is sufficient for most cases. This does not cause any problems with today's component, but the price of AD-converters for the first digital systems led to solutions, where multiplexers were used to feed several signals through one AD-converter.

Another issue is related to the fact that the quantification introduces noise depending on the number of bits used in the quantification. In analog systems signal noise is not a problem, because the noise can be filtered away. For digital systems, noise can be disturbing when two small signals are subtracted from each other. Analog systems on the other hand can have problems with zero point drift.

Uncertainties

Analog and digital systems have behavior that is qualitatively different. The continuity of signals in analog systems imply that it is possible to argue that behavior will be predictable in a region of normal operation at least with some level of accuracy. This is not possible for digital system as the Turing's theorem in mathematical logic states. The only way of predicting behavior of a digital system is to let it run and observe its behavior. An additional difficulty is quantification of the state space of a digital system, which means that two neighboring states may show qualitatively different trajectories.

These uncertainties imply that it hard or even impossible to predict execution times for software modules and thereby ensure that they will be shorter than the sampling time. It is also impossible in programmable systems to predict the path the execution will take. In practice this means that it is not possible to require certainty and predictability in the licensing of digital system. Confidence in digital I&C should be built on other arguments.

Requirements Specifications

The creation of requirements specifications is an important phase in the design of any system. The requirements specifications can be seen as a set of rules that should be true in defined situations. To prove that a system behaves correctly, it would be necessary to prove that the requirements are complete, consistent and correct (C_3). Completeness would imply that all possible situations are covered in the requirements, i.e. a proof that there are no situation exists, which has not been considered. Consistency would again imply that there are no conflicting requirements in the requirements specifications. If we consider the requirements specifications as an axiomatic system, then according to the Gödel's theorem in mathematical

logic, there are only two possibilities, either there are situations not covered by the requirements specification or there are conflicting requirements in the system. Correctness cannot be proven in practice, because in the licensing phase it is not possible to prove that a NPP will be constructed as the requirements specify. The comparison of different memory technologies in digital gives its high output performance in terms of accuracy.[16,17] So Digital IC Design much easier compare to Analog IC Design. These difficulties suggest that licensing requirements for digital I&C should not constructed from what may be considered necessary, but instead from what can be considered to deliver sufficient safety. In doing this, the principle of a graded approach to safety could be used to relieve the burden of proof for I&C in less important functions. In a realistic safety case for I&C it should be enough to consider event sequences, where risks are larger than defined rest risks for the NPP. This implies that some sort of quantification must be used for some I&C based scenarios.

Application and Platform

Digital I&C has introduced a separation between application and platform, in the sense that the application of a digital I&C system is created by a specialized programming language that executes a run time version of the application software. The platform comprises of hardware and system software designed at an earlier point of time. This solution has the benefit of making it possible to reuse the platform over different applications.

For analog I&C the application was built by physical interconnections between functional components of the selected hardware. The application software for digital I&C have similar functions, but the interconnections are built by software interconnections between modules of the platform.

The division into application and platform gives flexibility in implementing functions, but this flexibility may also be used to mix functions in unfortunate ways, for example by introducing unnecessary interdependencies. It is therefore important to use an intermediate step, I&C architecture design, between the functional design and the design of the application. In the I&C architecture it is important to ensure separation between functions and components to arrive at a clear structure in which safety classifications is reflected.

The I&C Design Process

The functional difference between analog and digital I&C are not very large. The application design is very similar in analog and digital systems. The largest difference between analog and digital is the introduction of two new design levels, 1) the platform design and 2) the architecture design. A well designed platform has taken a proper account of sampled time and discretized signals, but unsuitable architectures or application designs may still introduce problems. The design process of the platform software has in most cases to be considered as a black box, which means that very little or no structural evidence is available to establish confidence in the platform. This also means that an assessment of the I&C architecture by necessity is somewhat vague. What kind of confidence can be placed in claims of independence, spare capacity, execution times, self-diagnosing behavior and failure recovery?

The need for building confidence in a digital I&C platform depends on a possibility to open up the internal structures of the platform and the system software. In the competitive climate of early digital systems the vendors of digital I&C apparently did not want to do that, which seems to have enlarged distrust into the licensing process. The rapid development of digital I&C also introduced their own difficulties for example to decide when a modification of an existing platform made it necessary to redo some of the verification and validation (V&V) of the system software.

The Complexity of Digital I&C

The main difficulty in licensing digital I&C is the complexity of software based systems, because complexity makes any design process error prone. The dimension of the state space of a digital I&C, as characterized by its internal variables, may easily be hundreds of thousands', which means that it is practically impossible by testing ensure correct behavior even in a very small number of possible situations. In addition there is no structural assurance that state variables are not mutually interdependent. For analog I&C the dimension of the state space could be estimated in the count of relays and controllers,

which was large, but it still provided possibilities to approach in test programs, because analog components could be considered independent if not physically connected. An additional difficulty is that I&C itself makes a contribution to complexity, because a successful control system should have a similar complexity as the system it is supposed to control.[4] Design for simplicity can therefore be seen as the key for building a basis for licensing digital I&C. Simplicity can be achieved both in restricting the number of internal state variables.

Building a Safety Case for Digital I&C

It is not possible to provide hard proofs that digital I&C systems are able to deliver required services and will not show unintended behavior. However, by collecting information from the I&C design processes it should be possible to get structural information on state variables and their interconnections that can help in building the safety case. What kind of safety principles have been used in the design processes and how strictly have they been followed? Is it possible to claim that some typical design errors have been avoided? These questions can at least partly be answered by providing information on the management systems that have been used in the I&C design processes.[5] The second layer of information on interconnections is contained in the requirements specifications for the I&C platform, the I&C architecture and the I&C application. Additional information on how unwanted interdependence has been avoided by the use of safety principles can provide inputs to a modular testing program, which is targeted on demonstrating correct behavior for selected functions.

Requirements

Considering requirements placed on NPPs, there is a large body of experience available.[6] These requirements can be considered as a hierarchical system together with specific safety principles used in different parts of the design process. The reasoning should proceed according to standard risk assessment practices. What are the postulated initiating events (PIE), which form the design basis to be considered in NPP operation and how would they interact with the I&C? Using the safety principles of eliminate, separate, control and mitigate, it should be possible to build an argumentation that catastrophic events have been avoided with a large certainty.

For the I&C design corresponding functional and non-functional requirements are obtained in that process. These requirements should be collected to a system of requirements specifications that are used in initial phases of the I&C design. One may for example consider the need for procedures to collect evidence of safe behavior within different safety classes of the I&C. The problem is that the requirements specifications may contain contradictions and ambiguities, which however at least partly can be alleviated by a thorough analysis.

Functions

The I&C functions emerge as result of the requirements specifications for the NPP. The first step in implementing the I&C functions is to develop an I&C architecture with the selected I&C system. The architecture should reflect applied safety classifications to ensure independence between major I&C subsystems. In the architecture it is also possible to utilize failure protection built into selected I&C system and the platforms. It may be necessary to do pilot designs with two or more I&C systems to assess their suitability. Details of the design and decision making processes should be carefully documented to build both the design base and argumentations for the safety case.

The first step in building a safety case for digital I&C is to acknowledge the separation between application and platform. The requirements specifications for the application emanate from plant design, which means that functions have to be assessed in connection with a plant risk analysis. The easiest way of building confidence in the application is to use a plant simulator, where I&C functions in a first phase are simulated using their functional descriptions and in later phases by emulating the I&C system or connecting actual I&C cubicles to the simulated process. This also gives the possibility to experimentally verify a smooth recovery from I&C failures.

Design Threats

Already from the beginning it is important to identify types of failure modes that will be given a closer scrutiny in the design process. For the I&C this will mean investigations of possibilities for failure detection and management. Important failure types are failed sensors and control elements, failed

computational, communication and control room units, failures in power supplies, failures due to stressing environmental variables, etc. In most cases such failures can be abated with the principles of redundancy, separation and diversity. Many of the failure modes can be eliminated, isolated, controlled or mitigated by selecting a suitable I&C architecture, by standard functions of the platform, by specialized application programming and/or by good software programming principles.

The selection of failure modes to be considered in I&C design should apply similar principles as the consideration of PIEs for the NPP itself. This means for example that both external and internal failure modes of the I&C should been taken in account. Another distinction in failure modes is to consider natural threats, which are due to nature and resulting in equipment failure or human errors. A similar approach can be used for cyber threats that are the result of actions of intelligent adversaries.

Applied Safety Principles

The safety principles applied in the I&C design process are intended to make certain failure modes impossible or less likely. It would therefore be important to explicitly document applied safety principles together with evidence that they have been followed. In addition it would be necessary to provide an account of the expected efficiency of applied safety principles.

One important safety principle to be applied is to avoid common cause failures by ensuring independence between safety precautions. Independence can in many cases be claimed to exist due to structural properties, such as locations in different rooms or buildings, different power supplies, different sensing devices and different control elements.

The principle of building barriers to protect the integrity and authenticity of software and data against human errors in modifications and intentional tampering is another important safety principle to apply. To what extent credit can be given to such protection within the I&C platform is a question to discuss. Considering threats for persistent software errors one source that is difficult to attend to, is the modifications that take place during the design process. If such modifications are not made with necessary care, there is a large risk that corrections of earlier design errors bring in new errors. Finally the principle of experience feedback from other similar I&C design projects is also an important safety principle to apply. This feedback should be broad enough to encompass in depth discussions with I&C vendors and their customers. If that experience is possible to quantify to some extent it would be very valuable for the safety case.

Risk Analysis

A typical division is to separate between deterministic and probabilistic risks analysis. In the case it is possible to use deterministic reasoning it is fine, but this may not be enough for really important safety functions. To some extent it is possible to build event and fault trees for various scenarios and to make rough calculations of their probabilities.[7] If it can be argued that the I&C functions are one order of magnitude more reliable than the physical components (valves, pumps), it should be possible to claim a satisfactory reliability for the I&C part of the safety function.

This may not be possible for the reactor protection system. One possibility is to use two diverse process systems, which may or may not be implemented with diverse I&C platforms. In the case one would need to integrate evidence from testing and operational experience together with the structural information that has been collected during the design process, it should be possible to introduce qualitative argumentation based for example on safety integrity levels. Qualitative arguments that rely on expert judgments with ordinal scales (e.g. small, medium, large) can also be used for valuing consequences and probabilities.

Using System Models

Automated testing has been proposed as a general policy to build confidence in software. This approach builds on the construction of a test oracle against which different versions of the designed software can be tested.[8] One possibility is to use executable requirements specifications that allow early impressions of obtained functionality of modules and subsystems. This approach is in line with recommendations by proponents for software development in iterative and evolutionary processes.[9] The modelling approach can be brought to a large

level of detail[10] or left on a functional level[11] to create increasing confidence in solutions.

Common Cause Failures

Finally the safety case should contain arguments on probability of common cause failures (CCF). A study[12] claims that CCFs in digital I&C actually are relatively rare. A combination of independence and diversity should make it possible to argue that that the likelihood of common cause failures has been reduced to a minimum.[13] Claims can build both on deterministic and probabilistic arguments. For example it is unlikely that two or more redundant, but non-diverse instrumentation channels would operate on exactly the same data streams, because of the discretization noise. It would also be possible to check the functionality of redundant channels, with respect to noise sensitivity, to provide evidence for correct functionality in a broader range of data streams. Functional independence with respect to power supplies, physical locations, cabling, common hardware, environmental conditions etc., should make it possible to claim a small likelihood for CCFs. For the highest safety classes it may still be necessary to use diversity in platforms or hardwired manual backup to provide convincing arguments that CCFs are unlikely.

Human Factors Engineering

One important part in establishing confidence in a I&C system is to ensure that the control room and control boards are understood and easy to use by the operators. This need was identified already in the analysis of the Three Mile Island accident. A recent report gives guidance on how this phase of confidence building could be carried out.[14] As in[18] Good Multipliers cab be design efficiently with good accuracy compare to digital counterpart. Failure analysis much easier in analog counterpart as the available technology is Mixed Signal IC Design technology which is definite now.[19,20]

Confidence Building

Confidence building should establish confidence both in the design processes and in the final product. This would imply comprehensive V&V of both subprocesses and intermediate products. As has been argued above, it is not possible to prove C_3 of the I&C design. Instead it would be important to have an early agreement on sufficient arguments for safety, because otherwise there is a large risk that the I&C design project will aim at a moving target and experience delays due to increasing production pressures and consequently an increasing likelihood of design errors.

Confidence building will, as discussed above take place in a parallel process with I&C design that put focus on a few issues at a time. In each area the argumentation will proceed from claims, which are supported by evidence. Some of the claims may consist of two or more sub-claims that in turn are supported by their own evidence.[15] There are several relative independent design processes in producing digital I&C systems. The plant design feeds the I&C application design with inputs and it should get back information on PIEs that have their source in I&C. This information should be used to build claims that design process is good enough.

The platform design process has usually taken place years before the NPP project, which means that it may be difficult to get information on its appropriateness. On the other hand if the I&C system vendor has collected suitable information from the design of the platform, it may be used in the confidence building process. Such information could be documentation of the management system together with information on standards and safety principles that have been used during design. Additional confidence building information may also be obtained from operational experience at facilities using the same platform.

A final important safety principle to apply in I&C design is to test the system against a plant simulator. Such a test bed may include data collection by which additional evidence for the function of applied safety principles can be tested. One such example is that the real time requirement for the software that could be checked both in the sampled time parts and in the event based parts of the software.

Final Arguments

A safety case should contain a chapter in which final arguments for safety is collected. The argument would be that the requirements on the NPP and its I&C are reasonably complete, consistent and correct, that a safe architecture has been implemented on a reliable platform, that the application design process

has been well structured and followed with regard to the applied safety principles and that V&V has been applied throughout the design process. This would lead to the claim that event sequences connected to failing I&C are below the rest risk set by the NPP design. To summarize, deterministic arguments can be obtained from structural evidence facilitated by the use of safety principles. Probabilistic arguments could claim that certain failures are of the order of the agreed rest risk based on structural evidence, testing, feedback of operational experience and engineering judgments. Finally testing against a full scope plant simulator would provide the final part of the arguments for safety.

Conclusions

The application of digital I&C has been hampered by unrealistic urges to provide evidence for completeness, consistency and correctness. There have also been disagreements on the timing of providing design documents and the extent of evidence needed before a I&C system can be considered safe. Confusion due to mixing of arguments regarding the safety of the application and of the platform has also made licensing more difficult. All this has led to delays and cost escalations both in NPP and I&C projects. It is apparent that the target for the safety case in many I&C projects has been moving during the design process. An unrealistic view of what a safety case is supposed prove, can at least in some sense be attributed to a deficient understanding of differences between analog and digital I&C. It seems that errors in early designs of digital I&C have had a negative influence on the trust between licensees and regulatory bodies. My hope is that realistic views on what should be a sufficient target for the safety case together with the use of explicit safety principles in the design projects, should be of help in making the time and efforts in licensing of digital I&C easier to predict.

References

1. B. Wahlström, Safety principles in I&C design, NPIC & HMIT 2015, Charlotte NC,2015.
2. IAEA, Nuclear Power Plant Instrumentation and Control: A Guidebook, TRS239,1984.
3. L. Bainbridge. Ironies of Automation, *Automatica*.1983;19:775-779.
4. R.C. Conant, W.R. Ashby. Every good regulator of a system must be a model of that system. *Int. J. Systems Sci*.1970;1:89-97.
5. B. Wahlström, C. Rollenhagen. Safety management – a multi-level control problem. *Safety Science*.2014;69:3–17.
6. B. Wahlström, A. Duchac. IAEA safety principles applied to NPP instrumentation and control, NPIC & HMIT 2015, Charlotte, NC, 2015.
7. O. Bäckström, J.-E. Holmberg, M. Jockenhövel-Barttfeld, M. Porthin, A. Taurines. Software reliability analysis for PSA, NKS-304, Nordic Nuclear Safety Research, 2014.
8. J. Valkonen, I. Karanta, M. Koskimies, K. Heljanko, I. Niemelä, D. Sheridan, R.E. Bloomfield. NPP Safety Automation Systems Analysis State of the Art, VTT Working Papers 94;2008. 10(10)
9. C. Larman, Applying UML and patterns; an introduction to object-oriented analysis and design and iterative development, Prentice Hall.2005.
10. J. Lahtinen, J. Valkonen, K. Björkman, J. Frits, I. Niemelä, K. Heljanko. Model checking of safety-critical software in the nuclear engineering domain. *Reliability Engineering & System Safety*.2012;105:104-113.
11. Jussi Lahtinen. Hardware failure modelling methodology for model checking, VTT-R-00213-14.2014.
12. EPRI, Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems, Report 1016731 (2008).
13. IAEA, Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, NP-T-1.5, 2009.
14. P. Savioja, Evaluating systems usability in complex work; development of a systemic usability concept to benefit control room design, VTT Science 57, 2014.

15. Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations, BEL V, BfS, CSN, ISTec, ONR, SSM, STUK, http://www.onr.org.uk/software.pdf. 2013.
16. CHANG, J., CHEN, Y., CHAN, W., *et. al.,* A 7nm 256Mb SRAM in high-k metal-gate fin FET technology with write-assist circuitry for low-VMIN applications. *In Proceedings of the IEEE International Solid-State Circuits Conference.* 2017, p. 206–208. DOI: 10.1109/ISSCC.2017.7870333.
17 RAKUS, M., STOPJAKOVA, V., ARBET, D. Analysis of bulk-driven technique for low-voltage IC design in 130 nm CMOS technology. *In Proceedings of the 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. 2017, p. 1–6. DOI: 10.1109/ICETA.2017.8102522
18. GODOY, P., DAWSON, J. L. Chopper stabilization of analog multipliers, variable gain amplifiers, and mixers. *IEEE Journal of Solid-State Circuits.* 2018; 43(10):2311–2321. DOI: 10.1109/JSSC.2008.2004328
19. SOVCIK, M., KOVAC, M., ARBET, D., et al. Ultra-low-voltage boosted driver for self-powered systems. *Microelectronics Reliability.*2018;80:155–163. DOI: 10.1016/j.microrel.2017.11.006
20. ARBET, D., KOVAC, M., NAGY, L., *et al.,* Low-voltage bulk-driven variable gain amplifier in 130 nm CMOS technology *In Proceedings of the 2016 IEEE 19th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS).* Kosice (Slovakia).2016;1–6. DOI: 10.1109/DDECS.2016.7482439.