Nuclear Engineering and Technology 53 (2021) 3694–3703

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Instrumentation and control systems design for nuclear power plant: An interview study with industry practitioners

Pooja Singh [a, *], Lalit Kumar Singh [b]

[a] Department of Mathematics, VJTI, Mumbai, India
[b] Department of Computer Science & Engineering, IIT (BHU), Varanasi, India

ARTICLE INFO

Article history:
Received 29 March 2021
Received in revised form
11 May 2021
Accepted 19 May 2021
Available online 31 May 2021

Keywords:
Instrumentation and control systems
Software and system safety
Dependability engineering
Safety critical systems

ABSTRACT

Instrumentation and Control systems (I&C) play a significant role in nuclear power plants (NPP) and other safety critical systems (SCS). We have conducted a rigorous study and discussions with experienced practitioners worldwide the strategy for the development of I&C systems to investigate the several aspects related to their dependability. We discussed with experienced practitioners that work on nuclear domain with the intention of knowing their approach, they use day-to-day for the development of such systems. The aim of this research is to obtain to provide guidance to those building I&C systems of NPP and have implications on state engineering licensure boards, in the determination of legal liability, and in risk assessment for policymakers, corporate governors, and insurance executives.

1. Introduction

Safety -critical applications are widely used in several critical domains such as Nuclear, medical, aerospace, defence [1]. These systems consist of heterogeneous software, hardware and firmware components. The main challenge for development of such systems is to meet high dependability requirements and to comply with international standards [2]. Therefore, developers and operators are required to obtain license before they are allowed to work on SCS that offers services directly or indirectly to the public or government. The organizations that develop SCS have to comply with international dependability standards.

I&C systems serve as 'central nervous system' of NPP [3]. Such systems contain various elements such as equipment, modules, subsystems, redundancies, systems, etc., through which the application senses basic parameters, monitors performance, integrates information, and makes automatic adjustments to operations of NPP as necessary. It also responds to failures and off-normal events to ensure the goals of such applications.

NPP contains several electromechanical dynamic components such as motors, pumps, valves that need to be operated in synchronized way to control thousands of plant parameters, such as neutron density, power density, temperatures, pressures, flow rates within the design limit to accomplish the overall objective of power production. This synchronization is performed by I&C systems [4]. To fulfil this objective, I&C systems retrieves the process parameters from several field sensors, compare these parameters with the respective set points, calculate the deviation of these parameters and send commands to actuate field devices to bring back the parameters within the set points. These systems also display relevant parameters through computer based human system interface (HSI) to inform operator about the status of the plant [5]. Apart, from this I&C systems are also safety systems to actuate the field devices, when control systems fail to control the parameters.

I&C system architecture has the following three primary functions.

1. *Measurement and surveillance capabilities* - to support monitoring or control functions [6]. For this, I&C systems like sensors or detectors interface directly with the physical process in the NPP and their status is communicated to HSI through communication systems. Such systems also interface with the decision-making applications. These measurement and display systems take judicious actions during all the operational phases of NPP.
2. *Automatic control* — I&C systems of NPP provides automatic control of main plant and several auxiliary or support systems [7]. They reduce the workload on the operators and control

* Corresponding author.
E-mail address: poojasingh1615@gmail.com (P. Singh).

https://doi.org/10.1016/j.net.2021.05.025

engineers and hence facilitate them more time for monitoring plant behavior.

3. *Safety functions* – I&C systems protect the NPP from any malfunction, by taking safe actions. It also responds to wrong manual actions. These safety functions provide instant automatic action(s) to protect both plant and environment [8,9].

I&C systems of NPP involve multidisciplinary expertise such as human factor engineering, system design, system simulation, software engineering, system integration, prognostics, and cyber security [10].

We have conducted in-depth interviews with industry experts, who work in the area of I&C systems of NPP, in order to investigate the practices and challenges involved to ensure their dependability to be used in SCS. We interviewed 19 industry experts from nuclear domain, 15 of them were having more than eleven years of experience, and 4 of them were having 5–6 years of experience in designing I&C for SCS. Collectively, these individuals have more than 200 years of experience in developing I&C systems of NPP. From education point-of-view, 8 engineers were post-graduated their engineering in Electronics and Communication, 7 engineers were post-graduated their engineering in Electronics and Instrumentation, and 4 engineers were post-graduated their engineering in Computer Science and Engineering.

This paper is organized as follows: first I&C systems are defined and a boundary set of such systems is offered. A system's boundary demarcates a limit to the system's internal components and processes. Boundary set includes boundary of the system as well as its interfaces. This boundary set is based on International Atomic Energy Agency (IAEA) definitions of I&C systems, augmented by the opinions of the consulted experts. Thereafter, an analysis of the interactions with these 19 experts was conducted to develop a set of themes identified for building I&C systems. In conclusion, we provide a set of recommendations for I&C system developers.

2. Research methodology

To meet the objective of our study, we apply qualitative research approach that includes in-depth systematic interviews [11] to conduct an investigation on I&C systems design for NPP.

The objective of our study is to understand the current industry practices for I&C design of NPP, for which we formulated research questions that will form a roadmap to meet our goals. The RQ are given in Table 1.We are concerned to know the main challenges involved to fulfill the functional and non-functional requirements of I&C of NPP (RQ1).

To answer this question, we need to first understand the main functions of CS (RQ1.1); how I&C systems consider safety measures (RQ1.2); what features should HSI contain (RQ1.3); how the design analyses of I&C systems should be performed (RQ1.4); and how to qualify new technologies and components.

Another important interest of concern is to know the certification process that the development organization is subject to become its systems in operation (RQ2). To answer this question, we need to identify the issues and challenges in relation to the safety and security (RQ2.1); and also, to identify the relationship between dependability and certification processes (RQ2.2).

3. Research framework

The research framework is designed in three steps: Planning and data collection; and Analysis. The steps are described below:

3.1. Planning and data collection

A qualitative research approach is used for investigation, in which informal discussions and interviews (email exchanges) with 19 industry experts were conducted [12]. The data was collected based on semi-structure interviews. The objective was to investigate and understand the process in depth within their real-life context. A qualitative research helps to understand the area of interest, explore it and put it in practice. This process also helps to improve the understanding continuously. A questionnaire was formulated to obtain the answers from the interviewers. The questionnaire covers the significant areas to fulfil the dependability requirements of I&C systems. The questionnaire was composed of open-ended and closed-ended questions, which were derived to answer all the RQ. Our set of questions were based on our experience working on SCS software, literature survey and formal or informal discussions with practitioners in conferences, meetings, collaborative projects, since many years. The interview guide is given in appendix A. The interviews were mix of video mode, emails and face-to-face. Video mode and face to face interview was of 40–60 min. Several significant responses were compiled through email communications also. Both the authors performed in-depth analysis of the recorded responses/notes to address the conflicts by discussing them in common forum, with proper reasoning. We presented a brief overview about the objective of our study to all the participants, before starting the actual interview process. All the interviews were recorded for analysis purpose.

Table 1
Research questions.

Research Questions	Aim
RQ1: What are the main challenges in relation to I&C systems design for NPP?	To devise a strategy to deal with those challenges in relation to design of I&C systems for NPP.
RQ1.1: What are the main functions of I&C systems?	To identify the resources and techniques, knowledge required to meet the functional requirements.
RQ1.2: How do I&C systems of NPP consider safety measures?	To identify issues and challenges of these approaches.
RQ1.3: What features should computer based human system interface contain?	To identify the issues those, arise in relation to implement those features.
RQ1.4: How should design analyses of I&C systems be performed?	To ensure the dependability requirements of I&C systems.
RQ1.5: How to qualify new technologies and components	To gain the confidence on new technologies and components to be used in I&C systems.
RQ2: What certification process is the development organization subject to?	To identify the certification process which the development organization is subject to become its systems in operation.
RQ2.1: What are the issues and challenges in relation to safety, security?	To identify the issues and challenges in relation to the safety, security?
RQ2.2: How does the certification process impact the dependability of I&C systems?	To identify the relationship between dependability and certification processes?

3.2. Analysis

The interesting and critical sections in the recorded interviews were marked according to the criteria defined by C. Roson [12]. All the questions were associated to one or more RQ, as listed in Table 2.

We examined each answer from different perspectives to conclude that how CS design are handled in industries. Many answers were similar. For analyzing the answers, we categorize them [13,14] based on the concept building technique. For example, the question Q16.1, "What system design philosophy do you use to fulfill the dependability requirements in CS?", we analyzed every 19 answers given by the industry experts, which are considered as different categories of CS design philosophy. In case, there were deviations in the answers of different respondents', those answers were discussed in common platform for a clear understanding till all the respondents' reach to a common platform.

3.3. Threats to validity

In this section, we discuss the threats to validity in relation to the research design and data collection. As described in Ref. [13], we consider four perspectives of validity and threats.

3.3.1. Construct validity

This validity tries to establish the correlation in between the theories behind the research and the observations [13]. We quantify the variable from our interview process that was containing open and close ended questions. We interviewed only those industry experts, who have a good experience in development of I&C systems, and the interview was conducted separately for each of the participant to ensure the anonymity. All the interviewees were also asked to let us know, if the question itself is not appropriate for the fulfillment of the objective. We could get different subjective answers from each of the interviewee due to the different way of interpretations, in this relation, which have been further discussed on common platform for convergence.

3.3.2. Conclusion validity

For conclusion validity, several literature studies and informal discussions with industry experts during occasional meets were executed to avoid formulating poor questionnaire. Each interview with industry expert was conducted separately to avoid cascading effect on the answers. Further we selected a mix of junior and senior experts, keeping an important consideration that juniors are more hunger of knowledge for current practices, more informal to have interactions with others. We also conducted chi square test to ensure the conclusion validity, for which we divided the sample data into category as discussed earlier. Then the numbers of points that fall into the interval are compared, with the expected numbers of points in each interval.

Table 2
Association between RQ and questions.

RQ	Open-ended questions	Close-ended questions
RQ1	Q19	
RQ1.1	Q10.1, Q11.1, Q12.1	Q3, Q4, Q5, Q6, Q7, Q8
RQ1.2	Q5.1, Q5.4, Q7.1, Q9	Q1, Q2, Q7, Q7.2, Q7.3
RQ1.3	Q10, Q11, Q12, Q13.1	Q5.1, Q5.2, Q5.3, Q5.4
RQ1.4	Q16, Q16.1, Q16.2, Q17	Q9.1, Q9.2, Q9.3, Q9.4
RQ2	Q13, Q20	
RQ2.1	Q13.2, Q14, Q18, Q18.1	Q15.2, Q15.3, Q15.1
RQ2.2	Q19.1, Q18.2, Q19	Q18.1, Q18, Q18.3

3.3.3. Internal validity

Threats to this validity are instrumentation, maturation, regression towards mean and selection. The instrumentation threat can occur when there is an issue with self-report measures given at different times. We have mitigated this threat through the use of retrospective pretesting. The pretest measures abilities or knowledge before information or skills are presented in a program and we have conducted a rigorous study and informal discussions with experts before we initiated our thinking for this interview study, to address this issue. As we have selected the sample for interview that suits to our objective, some of them were having good expertise of development of I&C systems, some were reliability and safety experts, there is no possibility of 'regression towards mean' threat.

3.3.4. External validity

We have conducted the interview session in a very systematic and unbiased manner. As we have already formulated the questionnaire based on our rigorous literature survey and informal interactions with many organizations, apart from which had participated in this study; there is not possibility of putting up biased questions. Also, each interview was interviewed independently to avoid the influential answers. We have chosen a mix level of industry experts. So, there is no possibility of external threat in our study.

4. Results and analysis

The analysis of the results against each research questions formulated, as mentioned in Table 1 is presented in this section. To address each research question, bottom-up approach is used; for example, to answer RQ9, we have formulated 4 RQ: RQ9.1, RQ9.2, RQ9.3, and RQ9.4. So, we answer these 4 RQ in order to answer RQ9. For this, informal discussions and interviews were conducted with 19 I&C engineers, as mentioned previously. The essence of these interactions was captured and a thematic analysis was performed. The identified themes are organized into the following sections. We started interviews with basic questions, such as:

Ques 1: "What is a Control System?"

Ans 1: "A control system is a system, which provides the desired response by controlling the output."

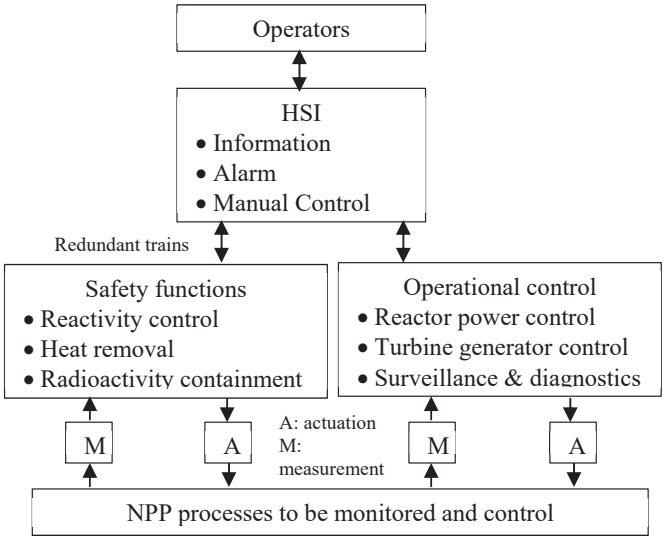

Fig. 1. Functional overview of NPP I&C.

Ques 2: "What are the main functions of I&C systems? What are the basic components in I&C of NPP?"

Ans 2: "The responses are summarized and mentioned in section 3-A."

4.1. Functions of CS (RQ1.1)

4.1.1. Functions

To keep the system parameters within design limits, accurate and reliable information about the parameters is needed, which is provided by the sensors. There can be diversified sensors depending on the type of parameters [15,16] that include temperature, pressure, level, flow rate, etc. Control systems compare the measurement of the plant parameters [17] with design set point and take corrective actions by controlling actuators based on the deviation from this set point. The values of process parameters are measured through sensors. Normalization of sensor signals [18] is necessary to process sensor signals in a uniform way, which is done in signal conditioning and data acquisition block [19]. Then signals can be processed in the normal way that includes scaling, linearization, filtering etc [20]. The result of the signal processing is used to control the actuator.

Analog I&C systems use analog voltages or currents and analog electronics to process the signals and to control the actuators. Digital I&C systems do the signal processing and control the actuators by means of computer processors, using a binary representation of the measured and controlled parameters. From the functional point of view both solutions are similar but from the physical point of view, the differences are significant. Fig. 1 shows the elementary I&C function in the context of the related process elements [21].

To ensure safe and reliable plant operation under any condition, I&C systems have to monitor several plant parameters and hence NPP I&C systems are complex. To understand the entire system, I&C are categorized according to its functions. These systems are commonly categorized in groups: Sensors; operational control, regulation and monitoring systems, safety systems, communication systems, HSI and actuators [22]. At the lower level, I&C systems can perform the functions: data acquisition, actuator activation, validation, arbitration, control, limitation, checking, monitoring, command, prediction, communication, fault/alarm management, and configuration management. As safety is the prime objective in nuclear domain, we asked the question as follows:

Ques 3: "How is the reliability and safety of I&C systems ensured? What preventive actions are considered in the design to meet the reliability and safety criteria?"

Ans 3: "The responses are summarized and presented in section 3-B."

4.1.2. Safety considerations in I&C systems (RQ1.2)

For the safe operation of NPP, several I&C systems do have high dependability requirements [8,9,23], for which the following design principles are applied.

1. *Specification of Performance requirements* – is necessary to ensure that these functions are achieved over the full range of measured variables to be accommodated, with the characteristics to produce the necessary output signal [24].
2. *Design for reliability* – of I&C systems important to safety is necessary to prevent undue challenges to the integrity of the plant physical barriers provided to limit the release of radiation and to ensure the reliability of engineered protective systems. Important aspects of the design for reliability are: single failure criterion, redundancy, diversity, independence [25–28].
3. *Fail safe criterion* – I&C systems must be designed such that their functions are more tolerant of expected failures of systems or components.
4. *Control of access* – I&C systems must be designed to prevent unauthorized access and also to reduce the possibility of errors caused by authorized person.
5. *Set point Validation* – I&C systems must be designed such that their functions must actuate to ensure safety do so before the related process parameter exceeds its safe value. An analysis is necessary to calculate the point at which the I&C system must act to accomplish this.
6. *Design for optimal operator performance* – is the practice of applying human factors engineering to minimize the potential for operator errors and limit the effects of such errors [29].
7. *Equipment qualification* - is a process for ensuring that the systems and equipment important to safety are capable of performing their safety functions.
8. *Quality in design and manufacturing* – of equipment important to safety is necessary to demonstrate that they will perform their assigned safety functions.
9. *Design for electromagnetic compatibility* - is necessary to ensure that installed systems and equipment will withstand the electromagnetic environment in an NPP, which can be done by making appropriate provisions for the grounding, shielding and decoupling of interference [30].
10. *Testing and testability* – I&C systems of NPP must provide a provision in the design that facilitates testing, calibration, and maintenance, and the establishment of programs to appropriately schedule, conduct, and learn from these activities [31].
11. *Maintainability* – I&C systems must provide a provision of additional redundancy to meet single failure criterion during the time when any component or subsystem is taken out for maintenance or testing.
12. *Documentation* – of I&C functions, systems and equipment is necessary to ensure the availability of sufficient and adequate information for safe operation of NPP.
13. *Identification* – of I&C functions, systems and equipment is necessary to ensure that these items are properly treated during all the cycles of NPP that includes design, construction, maintenance and operation.

Apart from these design principles, security aspects should also be considered to ensure that the constituent hardware and

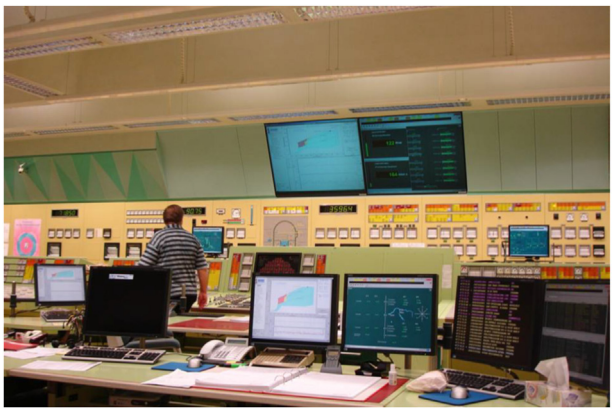

Fig. 2. Hybrid control room of NPP.

software are resistant to cyber threats.

By applying the above principles, some of the common design approaches that have emerged are functional isolation; redundancy; physical, electrical, and communications isolation; electrical noise; diversity; defense in depth; control of installation, maintenance and design change.

As HSI plays an important role for the overall safety of NPP, we asked the following question:

Ques 4: "What features should computer based human system interface contain?"

Ans 4: "The responses are summarized and presented in section 3-C."

4.1.3. Features of computer based HSI (RQ1.3)

HSI of NPP are computer based and provided to control and monitor its relevant systems and components [29]. The main features of HSI are graphic displays, mimic displays, signal trend display, alarm annunciation and display, event display, history display, diagnostics display and also to send commands to the field to control permissive actuators. The philosophies for operation and display may differ for different I&C platforms. A digital system can be combined with a conventional HSI by connecting conventional indication and control means via input/output devices to the system. This results in increased cost, since additional hardware becomes necessary. Where safety or availability requirements demand an alternate, workstation independent access to indications, alarms and controls, this approach is a viable solution. Control rooms featuring both kinds of HSI are regarded as hybrid control rooms as shown in Fig. 2.

HSI of NPP implements operatystems that include Safety Parameter Display Systems (SPDS); Core behavior surveillance and prediction, monitoring limit violations; Alarm filtering; Electronic procedures presentation; I&C equipment and process performance monitoring; Various diagnostics systems (e.g., vibration or loose part monitoring); Monitoring primary circuit radioactivity levels (e.g., iodine isotopes); Normal transient and/or steady state process supervision and coordination; Electronic documentation presentation; On-line risk analysis (generally not for control room use); Event cause analysis (generally not for control room use).

It is necessary to ensure that displays must not be hazy and overloaded in terms of number of elements in single screen or use of several colors; considering the limitation of human cognitive ability. Under abnormal conditions, the important information must be focused on the display so that operator can interpret the information correctly to take the relevant corrective actions.

It is necessary to ensure the integrity of the design before going for its realization. To understand the practices being followed to ensure the integrity of the design of I&C NPP systems, we asked the following questions:

Ques 5: "How you ensure the design integrity of I&C systems"

Ans 5: "To prove the integrity of I&C systems, we perform the design analysis". The method to perform the design analysis are summarized and mentioned in section 3-D."

4.1.4. Design analyses (RQ1.4)

A top-down approach is followed in the design of I&C systems where refinements are done continuously. It is advised to proceed as long as possible with a system independent functional design, where the hardware platform and software are selected after the design has stabilized. The system design should provide the detailed design requirements.

Design analyses that are commonly done for I&C systems of NPP are I&C system redundancy analysis, common cause failure analysis, common mode failure analysis, EMC design analysis, defense in depth analysis, diversity analysis, software reliability and safety analysis, failure mode analysis, FMEA, FMECA, FTA. HIS and HFE analysis, analysis of software design and development process, analysis of security features, analysis of configuration control, performance analysis, signal accuracy analysis [32,33].

As I&C systems of NPP are distributed in nature, where processing nodes are communicating among themselves to perform the overall functionality of the system. The processing nodes are located remotely and hence it is mandatory to address the security concerns, considering the safety objectives. To know the issues and challenges we asked the following question:

Ques 6: "How do you ensure the safety and security? What are the issues and challenges that are being faced to achieve this?"

Ans 6: "The issues and challenges are summarized and presented in section 3-E."

4.1.5. Safety & Security: Issues and Challenges (RQ2.1)

It has been observed that I&C systems have been widely increasing in other industries as compare to nuclear industry, especially in safety applications. The reasons are less confidence on the dependability of the NPP systems, lack of well-defined licensing practices, lack of technical knowledge and management issues. Some of the major issues associated with the application of I&C technologies are: the defense in depth principle, protection against CCF, software verification and validation, cybersecurity, configuration management, safety assessment in the licensing process, network communication [1,9,10,25]. The five measures that have been identified for defense in depth in an NPP are listed below.

1. Prevent system failures and deviations from normal operations.
2. Detect and intercept deviations from normal operating states to prevent anticipated operational occurrences from escalating to accident conditions.
3. Control the consequences of accident conditions.
4. Confine radioactive material in the event of severe accidents.
5. Mitigate the consequences of radioactive release.

In I&C designs, different systems are developed to support each of the defense, as shown in Fig. 3, where monitoring, ESF actuation, shutdown system are safety systems and control systems are safety related systems. There must be strong independence between safety systems and safety related systems. The architecture of current I&C systems is fundamentally different from that of traditional I&C, as shown in Fig. 4. In traditional approaches, more components support only one defense and hence single failures generally affect only one level of defense. However, exceptionally, failure of one measurement channel might affect multiple level of defense.

As several I&C systems that are important to safety needs to be certified by regulatory authority, the dependability aspects need to be ensured according to the regulatory requirements. To meet this, there may change in the design or implementation. To clarify, we posed the following question:

Ques 7: "What is the impact of certification process on dependability"

Ans 7: "The responses are summarized and presented in section 3-F."

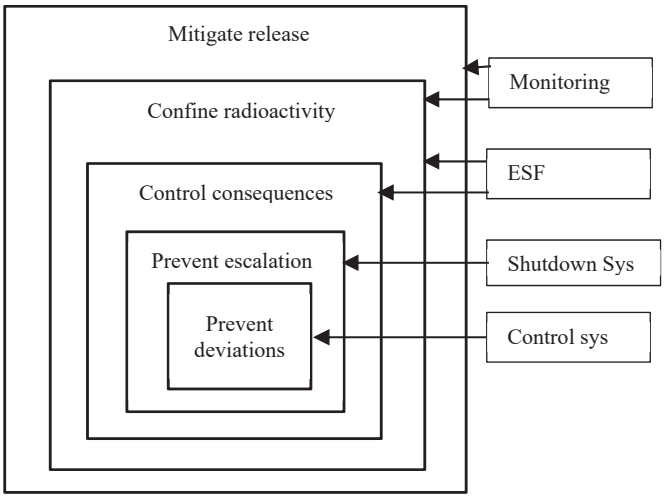

Fig. 3. Relationship in I&C system and defence in depth.

4.1.6. Impact of certification process on dependability (RQ2.1)

I&C failures at some selected plants are shown in Fig. 5. It can be seen that the contribution of failure of I&C systems ranges from 15 to 22% of the total number of failures. This data has been identified by an IAEA ASSET mission in designated WWER-1000 units. As I&C systems are nervous system of NPP, should meet high dependability requirements, which can be possible through certification process.

The certification process performs a rigorous verification and validation of the system development life cycle to ensure the high dependability of I&C systems.

5. Issues and challenges

Based on the interviews, analysis of the responses, and discussions held with practitioners, several significant issues have been identified. This section discusses all of them. The list is not exhaustive and will evolve with technological advancements and change of other factors.

1. *Transformation of analog to digital systems* – Traditional analog systems of NPP are being transformed into digital systems because of several benefits: more accuracy, absence of drift, high-capacity logs, ease of implementation of complex features, fault diagnosis, fault correction, capture the data correlation from many system components and their interfaces, useable Human Machine Interface (HMI), etc. However, digital technology makes the use of software components and even a small software module can exhibit substantial complexity to make a complete verification of its correctness practically impossible and hence the missing scenarios, during the V&V process, may get executed that make the system to possible attack and compromise. In this case, redundancy of the software will not serve the purpose, as the software is identical in each of the redundant channels. Even software diversity may also not work, when the ultimate cause of error is in the software requirements specification.
2. *Increasing chip density* - The use of deep sub-micrometre technologies can have a negative impact on long term reliability of electronic equipment. They tend to be more susceptible to single event effects. A single event upset does not permanently damage a transistor's or circuit's functionality, unlike the case of single event latchups, single event gate ruptures, or single event burnouts, however, re-initializing the system would erase all deleterious effects of the single event upset. The level of integration has the impact on the following two areas, due to electromagnetic compatibility (EMC):
   (i) Increased electromagnetic emissions due to increased operating frequencies and transient currents, as well as decreased switching times.
   (ii) Increased electromagnetic susceptibility: supply voltage reduction; reduced noise and delay margins

   Considering 1 and 2, a particular care must be taken while integrating new technologies.
3. *New Platforms* –The International Electrotechnical Commission (IEC) is preparing a standard dedicated to complex electronic components (CEC) to address many aspects such as guidance for analysis, selection and use of pre-developed CEC, rules for design phases, procedures for CEC modification and configuration control, guidance for the selection and use of software tools used to design and verify CEC. However, many issues are still open such as development of hardware and software qualification methods for FPGA, the use of formal methods for complex designs, can reverse engineering be feasible and how to find criteria for a repeated design.
4. *HMI* – Functions between humans and machine are likely to get changed during the upgradation of I&C systems, which can significantly impact the crew coordination, standard procedures, checklists, training and information. Hence, it is necessary to first upgrade the changes in the simulator, impart trainings to the operators and then gradually execute the change in the control room. Also, the changes should be properly planned after doing the impact analysis that include function analysis, performance requirements, etc, for which the existing equipment is used and for which the new equipment will be used. Noticeably, increased automation poses many challenges and can lead to deteriorated performance due to change of roles, responsibilities, workload, skills required, lack of training on add on automated functions, deterioration in operator awareness of overall plant operations, human error because of wrong assumptions regarding operating modes of the system. Also, there can be significant impact on replacing the obsolete components. The new component may not have all the inherent properties of the old component.
5. *New component and technologies qualification* – According to the regulatory guidelines, certain components and technologies import to safety, must be qualified to demonstrate their safety requirements, before putting them in use in nuclear applications that consists of: qualifying the suitability of component or product; conformance of the correctness evidence; proper documentation for safety. Many times, due to economical and availability reasons, commercial components are used in I&C systems of NPP. Functional qualification of such components is difficult because commercial development processes may be less well controlled or less transparent. Programming codes are also not shared for performing safety analysis. Proper documents are also not shared to complete V&V process more rigorously. Therefore, qualification of such components relies more on validation. However, designing effective test cases for 100% code coverage is not possible.
6. *Code reusability* – Generally, software developers use the existing code to build new software for similar or new systems. However, it poses many challenges and issues for safety applications. A well-documented example for such evidence is the loss of Ariane-5 launch vehicle [34]. This launch vehicle was destroyed because a high-quality software module from Ariane-4 was reused without fully confirming that the software would properly respond to the input values in the new Ariane-5 application. There are many more such examples.

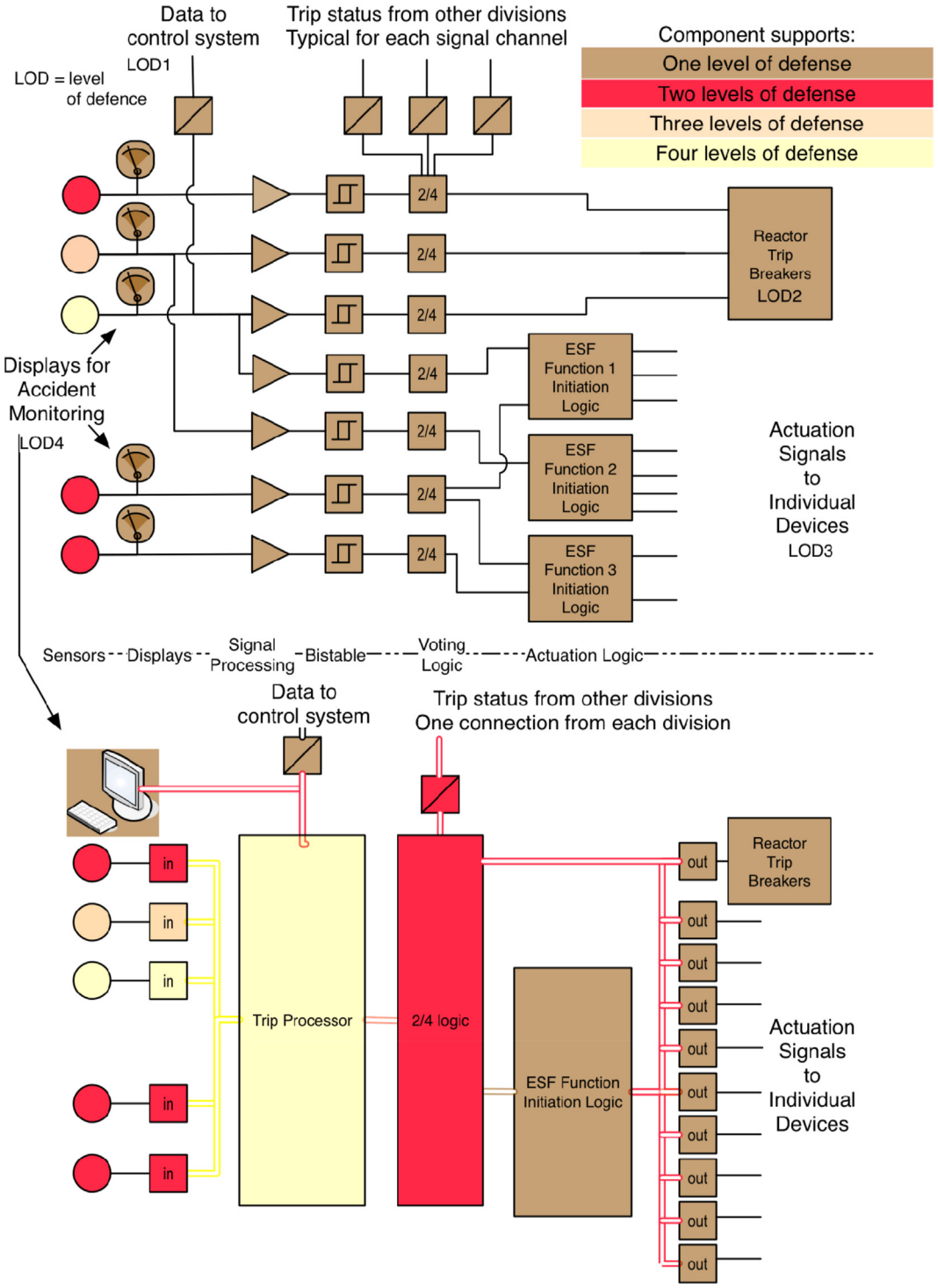

Fig. 4. Traditional vs Current I&C systems of NPP.

7. *Issues related to reliability, safety, and security* – Digital I&C has been adopted relatively slowly in the nuclear industry, especially in safety critical systems. This occurred generally due to the lack of confidence in the reliability of programmable devices, licensing uncertainty and the lack of well-defined licensing practices, cost and schedule, workforce knowledge, management and employee acceptance, and so on. Some of the major issues are cybersecurity, configuration management, V&V of software, addressing common cause failures.

6. Summary of themes and conclusions

This study posed two research questions. The first was "what are the main challenges in relation to I&C systems design for NPP?" to answer this question, five research questions were formulated, as mentioned in Table 1tbl1 and to answer these questions, a collection of experienced I&C engineers was interviewed. The second was formulated as "what certification process is the development organization subject to?" We formulated two research questions to answer this question, as mentioned in Table 1.

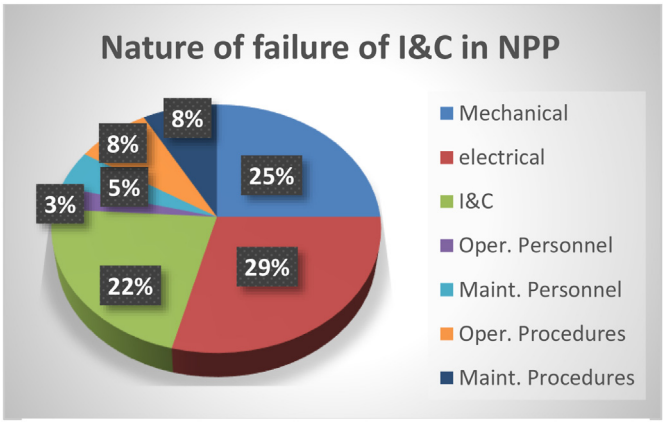

Fig. 5. Nature of failures at a selected NPP.

The answers given be interviewees were analyzed to derive themes. To summarize, some of the key-derived themes pertaining to I&C systems of NPP are as follows.

1. *Approach to implementation* – I&C systems of NPP should consider the safety features that include fail safe criterion, control of access, set point validation, equipment qualification, diversity, common cause failures, testability, and maintainability. To implement the upgrades, phased approach should be used to change the control room and associated I&C systems. Phased I&C upgrades using existing operator interfaces, followed by changes to upgrade the operator interfaces, and also the phased approach using system level changes to both the I&C equipment and associated operator interfaces at the same time.
2. *There is not universal standard* – There is no universal standard to develop I&C systems and changes with the criticality of the system. System analysts, safety experts need to play an important role in carrying out the activities during each of the system development life cycle. The organization should have its own standards and guidelines that can be based on the existing related standards, development experience and plant operating experience.
3. *Reliability requirements* – Safety related of I&C systems of NPP do have high reliability targets: 99.999%. I&C systems contains software and hardware components/systems. As the failure mechanism of hardware differs with that of software, hardware and software reliability models must be used accordingly to quantify the reliability of the overall system. More than 200 software reliability models are available, which so have different failure distributions. Hence, it requires a technical competency to understand the failure distribution of the target system to choose the software model wisely.
4. *Safety, security* – I&C systems of NPP do have high safety and security requirements. However, it is difficult to achieve due to involve in software. To ensure the dependability requirements of software, it should be developed using a systematic software development life cycle and using international design standards. Online testability feature should be incorporated into the software design. Software testers should be able to generate test cases wisely in concurrence with system designer.
5. *Conventional testing* – can be used to test I&C systems that include factory acceptance testing, site validation, etc.
6. *Verification and Validation* – I&C systems of NPP must got through rigorous verification and validation process to ensure the integrity of system. A proper V&V plan should be developed and submitted to the regulatory body for review, before going through the process. Then a system validation procedure should be developed by the system designer, which should contain all the test scenarios, keeping in view of 100% code coverage. The test scenarios should be discussed with the stakeholders for addition/updation.
7. *Software development on open-source platform* – Software components of I&C systems should be developed on open-source platform such as Linux, as it is less prone to virus attacks. Moreover, the source code is available to perform analysis to ensure the dependability.
8. *Tool sets differ widely by project and as defined in the scope of the work* – tools can be misused and are often mistrusted. Each tool should undergo suitability analysis and should be certified by the authorized body.
9. *Documentation* – Documentation should be proper throughout each phase of system development life cycle for testing and maintainability. It helps in proving the integrity of the design to the regulatory body and facilitate the verification and validation activities.
10. *Design analysis* – Top-down approach should be followed for design analysis of I&C systems of NPP. This approach should also be used for operation and maintenance. Based on the plant process description, the functional analysis contains the definition of all the needed functions for operation and maintenance in different plant conditions (normal and abnormal). The analysis of the "process-oriented" functions can be done in a top-down approach, where the top level represents the most general or fundamental objectives of the plant (generation of electrical power, protection from radiological hazards). The lowest level represents very detailed functions, which will be implemented, among others, in the I&C system or will be performed by an operator.
11. *Defense in depth* – I&C systems of NPP should follow defense in depth philosophy. The overall plant safety approach involves a defense in depth strategy such that multiple independent barriers must fail before the public is exposed to radiation. I&C systems are common to all of these barriers; therefore, the I&C design must be carefully considered to ensure that it does not weaken the overall defense in depth concept. This is usually accomplished by an examination of common cause failure vulnerabilities in the I&C system. The application of diversity is an important strategy to cope with common cause failures. Signal and functional diversity are commonly provided within safety systems to deal with the possible design or analytical errors that affect individual functions.

The themes can be expanded into set of best practices for those building I&C systems, by state engineering licensure boards, in the determination of legal liability and in risk assessment for policy-makers, corporate governors, and insurance executives.

The stated themes can be included in the list of best practices, for example, by using them as benchmark for expansion by the experienced team of practitioners. Then the expanded benchmark set would be communicated to a larger group of experienced practitioners. Thereafter, refinements may be done with common discussions to create a handbook of best practices and in the development of standards [35]. Finally, our study also facilitates in the determination of legal liability and in risk assessment to take policy decisions.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Interview Guide Appendix A

General Questions		Relation with RQ
Q1	What are the control systems? What control systems are being using in NPP?	RQ1.1
Q2	Is there any classification technique for I&C systems of NPP?	RQ1.1, RQ1.2, RQ1.4
Q3	What are the main functions of I&C system of NPP?	RQ1.1
Q4	How reliability and safety criteria is ensured?	RQ1.2, RQ1.5, RQ2.1
Q5	What are the issues and challenges involved in ensuring reliability and safety?	RQ1, RQ1.2, RQ1.4, RQ1.5, RQ2
Q6	How you ensure the security requirements in case of distributed I&C system?	RQ2.1, RQ2.2
Q7	What are the design characteristics of I&C system?	RQ1.2, RQ1.3, RQ1.4, RQ2.1
Q8	What are the issues and challenges in relations to safety, reliability, and security?	RQ1, RQ1.3, RQ1.4, RQ1.5, RQ2
Q9	How the integrity of the system design is ensured?	RQ1.4, RQ2
Q10	What are the qualification criteria of the components to be used in NPP systems?	RQ2
Q11	What is the regulatory requirements of I&C systems?	RQ2
Q12	What certification process is the development organization subject to?	RQ2
Q13	How the component-of-the-shelf are used in I&C systems?	RQ1.2, RQ1.5, RQ2.1
Q14	What is the suitability criteria of component-of-the-shelf?	RQ1.2, RQ1.5, RQ2.1
Q15	What system development life cycle is being followed?	RQ1, RQ2
Q16	Does any changes required to fulfil the regulatory requirements?	RQ2
Q17	How important is HSI in achievement of safety requirements?	RQ1.3
Q18	What is fail safe criterion?	RQ1.2, RQ1.4
Q19	What are the characteristics of HSI?	RQ1.2, RQ1.4
Q20	How set points of the signals are validated?	RQ1, RQ1.4
Q21	What human factor engineering processes are adopted?	RQ1.2, RQ1.4
Q22	How to ensure that installed systems and equipment will withstand the electromagnetic environment in an NPP?	RQ1
Q23	How testability of the system is ensured?	RQ1
Q24	What are the important documents that need to prepare in the development of I&C system?	RQ1.4
Q25	What challenges are being faced while transforming analog systems to digital systems?	RQ1
Q26	How EMC and EMI are ensured?	RQ1
Q27	How the systems are updated or transformed into the new platform when they become obsolete?	RQ1
Q28	How vendors are being selected in case already available component is used?	RQ1, RQ1.4, RQ2
Q29	What are the failure modes of the systems? How are they identified?	RQ1.2, RQ1.4, RQ2
Q30	What is the difference between traditional and current I&C systems of NPP?	RQ1
Q31	How control room systems are designed?	RQ1
Q32	What is simulator?	RQ1.1, RQ1.3
Q33	What is the validation plan?	RQ1, RQ1.4, RQ1.5
Q34	What are the review techniques?	RQ1, RQ1.4, RQ1.5
Q35	What measures are taken in case of any deviation during validation process?	RQ1
Q36	What parameters you display in the alarm windows of control room?	RQ1.3
Q37	What is the disadvantage of inspection test?	RQ1
Q38	How common cause failure is addresses?	RQ1
Q39	How you test the system before deployment?	RQ1
Q40	What is FMEA?	RQ1.2, RQ1.4, RQ1.5
Q41	What is FMECA? How is performed?	RQ1.2, RQ1.4, RQ1.5
Q42	What is FTA?	RQ1.2, RQ1.4, RQ1.5
Q43	How you measure the quality attributes of the system?	RQ1.4
Q44	How do you find bugs in the system?	RQ1
Q45	How the code is being reused?	RQ1
Q46	How you ensure the performance requirements?	RQ1, RQ2.1
Q47	How you perform timing analysis?	RQ1.4
Q48	How do you go for online testing?	RQ1.4
Q49	When you go for FMEA or FMECA?	RQ1.2, RQ1.4, RQ1.5
Q50	What is advantage of FTA?	RQ1.2, RQ1.4, RQ1.5

References

[1] L.K. Singh, H. Rajput, Dependability analysis of safety critical real-time systems by using petri nets, IEEE Trans. Contr. Syst. Technol. 26 (2018) 415–426.
[2] A. Ruiz, G. Juez, H. Espinosa, J.L. de la Vara, X. Larrucea, Reuse of safety certification artefacts across standards and domains: a systematic approach, Reliab. Eng. Syst. Saf. 158 (2017) 153–171.
[3] L.K. Singh, G. Vinod, A.K. Tripathi, Design verification of instrumentation and control systems of NPP, IEEE Trans. Nucl. Sci. 61 (2014) 921–930.
[4] V. Kumar, L.K. Singh, P. Singh, K.V. Singh, A.K. Maurya, A.K. Tripathi, Parameter estimation for quantitative dependability analysis of safety-critical and control systems of NPP, IEEE Trans. Nucl. Sci. 65 (2018) 1080–1090.
[5] Paulo V.R. Carvalho, Isaac L. dos Santos, Jose Orlando Gomes, Marcos R.S. Borges, Stephanie Guerlain, Human Factors Approach for Evaluation and Redesign of Human–System Interfaces of a Nuclear Power Plant Simulator, 29, Displays Elsevier, 2008, pp. 273–284.
[6] F. Di Maio, P. Secchi, S. Vantini, E. Zio, Fuzzy C-means clustering of signal functional principal components for post-processing dynamic scenarios of a nuclear power plant digital instrumentation and control system, IEEE Trans. Reliab. 60 (2011) 415–425.
[7] V.S. Volodin, A.O. Tolokonskii, Concept of instrumentation of digital twins of nuclear power plants units as observers for digital NPP I&C system, in: Journal of Physics: Conference Series 1391 012083, Bratislava, Slovakia, Aug 26-29, 2019.

[8] V. Kumar, L.K. Singh, A.K. Tripathi, P. Singh, Safety analysis of safety critical systems using state space models, IEEE Software 34 (2017) 38–47.
[9] V. Kumar, L.K. Singh, A. K Tripathi, Transformation of deterministic models into state space models for safety analysis of Safety Critical Systems: a Case study of NPP, Ann. Nucl. Energy 105 (2017) 133–143.
[10] Raj Kamal, Lalit Singh, Babita Pandey, Security analysis of smart grids: successes and challenges, IEEE Consum Electron Mag 8 (2019) 10–15.
[11] R.B. Svensson, T. Gorschek, B. Regnell, R. Torkar, A. Shahrokni, R. Feldt, Quality requirements in industrial practice - an extended interview study at eleven companies, IEEE Trans. Software Eng. 38 (2012) 923–935.
[12] C. Robson, Real World Research, Blackwell, 2002.
[13] C. Wohlin, P. Ruseson, M. Host, C. Ohlson, B. Regnell, A. Wesslén, Experimentation in Software Engineering: an Introduction, Kluwer Academic, 2000.
[14] P. Runeson, M. Host, Guidelines for conducting and reporting case study research in software engineering, Empir. Software Eng. 14 (2009) 131–164.
[15] M.L. Cummings, F. Sasangohar, K.M. Thornburg, Human-System Interface Complexity and Opacity Part I: Literature Review, A Technical Report Prepared for NRC, HAL2010-01, 2010.
[16] Kushal D. Badgujar, System science and control techniques for harnessing nuclear energy, Syst Sci Contr Eng 4 (2016) 138–164. Taylor and Francis.
[17] O. Riabenko, V. Tymoshchuk, D. Poplavskyi, O. Halych, Methods of automated full-scale measurement of wave parameters in water reservoirs of pumped storage power plants, in: IEEE 7th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine, 154-157, 2020.
[18] M. Liu, L. Liu, H. Song, Y. Hu, Y. Yi, F. Gong, Signal estimation in underlay cognitive networks for industrial internet of things, IEEE Trans Ind Inform 16 (2020) 5478–5488.
[19] W. Lu, T. Dai, S. Xia, Binary matrices for compressed sensing, IEEE Trans. Signal Process. 66 (2018) 77–85.
[20] S.J. Julier, J.K. Uhlmann, Unscented filtering and nonlinear estimation, Proc. IEEE 92 (2004) 401–422.
[21] IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants, 2016.
[22] J.W. Crandall, M.L. Cummings, M. Della Penna, P.M.A. de Jong, Computing the effects of operator attention allocation in human control of multiple robots, IEEE Trans. Syst. Man Cybern. Syst. Hum. 41 (2011) 385–397.
[23] Pooja Singh, Lalit Singh, Impact analysis of change in component reliabilities in safety critical systems, Qual. Reliab. Eng. Int. 35 (2019) 2051–2065.
[24] Pramod Kumar, Lalit Kumar Singh, Chiranjeev Kumar, Performance evaluation of safety-critical systems of nuclear power plant systems, Nucl Eng Technol. 52 (2020) 560–567.
[25] P. Singh, L.K. Singh, Reliability and safety engineering for safety critical systems: an interview study with industry practitioners, IEEE Trans. Reliab. (2021), https://doi.org/10.1109/TR.2021.3051635.
[26] P. Singh, L.K. Singh, Engineering education for development of safety-critical systems, IEEE Trans. Educ. (2021), https://doi.org/10.1109/TE.2021.3062448.
[27] P. Singh, L.K. Singh, Reliability and safety engineering for safety-critical systems in computer science: a study into the mismatch between higher education and employment in Brazil and India, IEEE Trans. Educ. (2021), https://doi.org/10.1109/TE.2021.3057611.
[28] Pooja Singh, Lalit Singh, Verification of safety critical and control systems of nuclear power plants using petri nets, Ann. Nucl. Energy 132 (2019) 584–592. Elsevier.
[29] Y. Lin, W.J. Zhang, A function-behavior-state approach to designing human-machine interface for nuclear power plant operators, IEEE Trans. Nucl. Sci. 52 (2005) 430–439.
[30] M. Štumpf, G. Antonini, I.E. Lager, G.A.E. Vandenbosch, Pulsed electromagnetic field signal transfer across a thin magneto-dielectric sheet, IEEE Trans. Electromagn C. (2021), https://doi.org/10.1109/TEMC.2021.3056484.
[31] Y. Jia, M. Harman, An analysis and survey of the development of mutation testing, IEEE Trans. Software Eng. 37 (2011) 649–678.
[32] W. Lohmiller, J.-.E. Slotine, Control system design for mechanical systems using contraction theory, IEEE Trans. Automat. Contr. 45 (2000) 984–989.
[33] L.I.U. Guo-Ping, Jian Sun, Z.H.A.O. Yun-Bo, Design, analysis and real-time implementation of networked predictive control systems, Acta Autom. Sin. 39 (2013) 1769–1777.
[34] European Space Agency, Ariane 5 Flight 501 Failure, Ariane 501 Inquiry Board, 1996.
[35] P.A. Laplante, B. Kalinowski, M. Thornton, A principles and practices exam specification to support software engineering licensure in the United States of America, Software Qual. Prof. 15 (2012) 4–15.