International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 4, April-2015, pp: (284-291), Impact Factor: 1.252, Available online at: www.erpublications.com

Enhancing Reliability of Digital Instrumentation and Control Systems

Hany Sallam[1], E. A. Eisawy[2]
Operation safety Department and Human Factors
Nuclear and Radiological Regulatory Authority

Abstract: Instrumentation and control I&C systems play an important role in ensuring the safety of NPPs by providing functions such as monitoring, control, protection, and mitigation. The I&C systems have an important role in protecting systems, structures and components from threats that could occur as a result of certain failure situations. A state-of-the-art digital instrumentation and control system using microprocessor technology provides replacement of older, existing instrumentation and control systems that contain obsolete components. Digital I&C systems are characterized by their increased flexibility, higher availability, and lower cost. But, on the other hand digital I&C systems may be more vulnerable to common cause failure CCF since they include software and hardware components whose failure may affect multiple functions. It is well known that CCF is a major drawback, which weakens reliability and consequently threatens safety of digital I&C systems. The reliability of digital system and its associated subsystem depends on the reliability of processing software and hardware. This paper proposes extending the levels of defense-in-depth and diversity to a new level, this level is the logic processing to defense CCF of digital components. Based on the extended defense-in-depth and diversity, redundancy, and independence a new more reliable I&C architecture is proposed.

Keywords: I&C systems, Reliability, Diversity, Defense-in-depth, common cause failure.

1. Introduction

While digital instrumentation and control systems are software based systems, Software defects may remain hidden for long periods after a product has been in general use, and failures may occur without any advance warning when a particular execution path is exercised. Such latent software faults may be triggered from data which depend on transients of the plant process [1]. About 40% of the world's operating reactors have been modernized to include at least some digital I&C systems. Most new plants also include digital I&C systems [2]. Typically, modernization of a digital I&C system is not limited to simply implementing the functionalities of the original analog system by digital means. Digital systems provide many additional features and functionalities, which should be considered for improving system reliability, availability, and overall system safety [3]. Digital computer systems are used in I&C systems important to safety to perform functions of protection, data acquisition, computation, control monitoring and display [4]. If properly designed, they can offer the advantages of improved reliability, accuracy and functionality in comparison with analog systems. The computer system may take many forms, ranging from a large processor supporting many functions to a highly distributed network of small processors devoted to specific applications [5]. Computer systems may be used to advantage in detecting and monitoring faults internal and external to plant systems and equipment important to safety.

Also, digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems. I&C systems with the highest responsibility for nuclear safety will require the best quality and reliability. Safety systems are the most responsible for nuclear safety. The reliability requirement is the highest among other requirements such as availability and quality [2]. Three features of digital I&C systems are distinctive. First, a digital I&C system has more connections among its many components and is simply more complex than its analog predecessor. Second, the digital system is more dependent on software. Third, the overall dependence on computers raises the importance of cyber security [6]. High reliability and low frequency of maintenance shall be mandatory for all systems. This is the result of adequate system design by introducing redundancy, diversity and physical isolation, in addition to the use of highly reliable components for each functional unit. One of the most significant basic design principles through which safety is incorporated into the NPPs is defense-in-depth. This principle involves the provision of consecutive and independent barriers that protect against the identified threats. Defense-in-depth principle leads to the application of diversity, separation and redundancy in systems and components to provide protection from random failures. In digital I&C systems, the possibility that a CCF can undermine safety is one of the major issues discussed in the licensing process. A number of the defense-in-depth measures applied to the design of I&C systems to help in mitigating the effects of CCF [1].

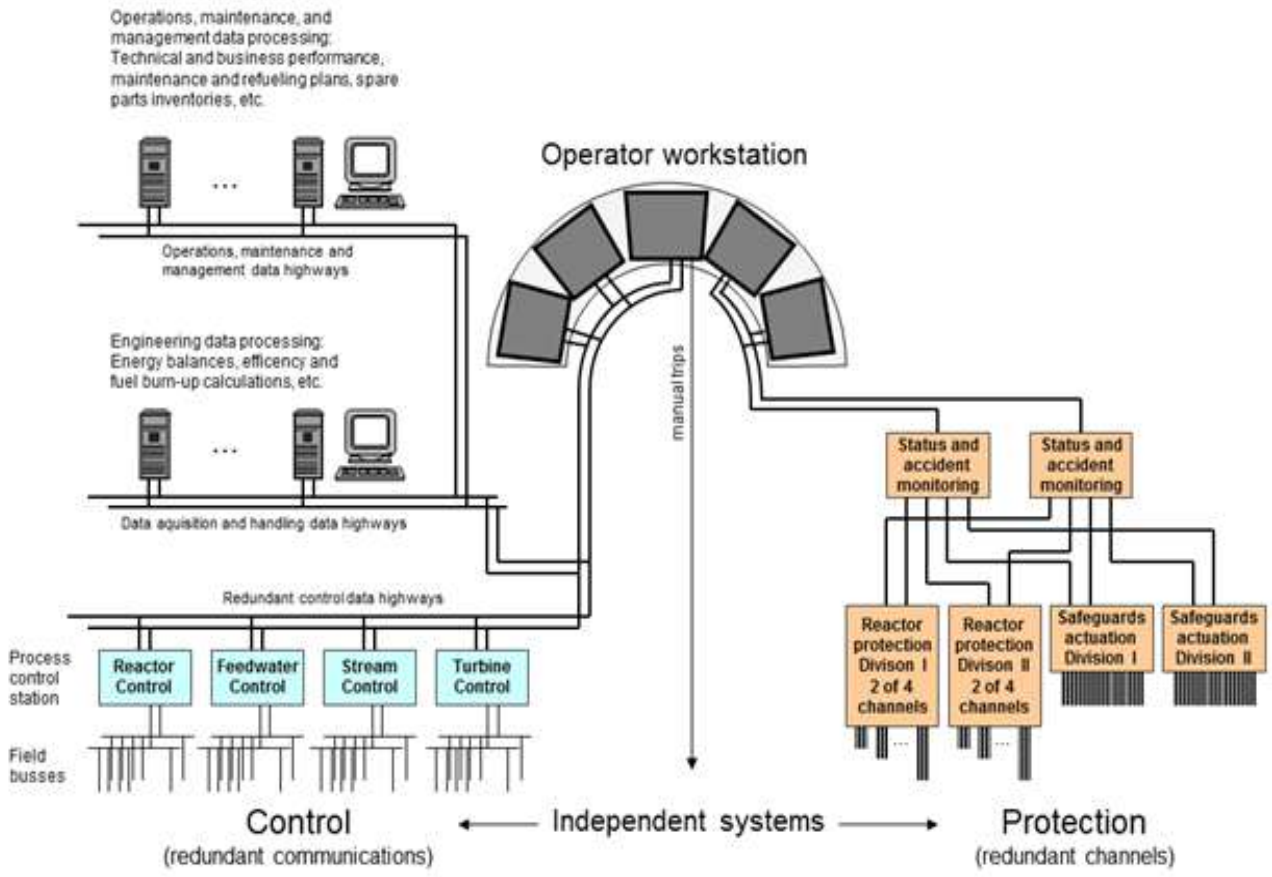

Fig.1, I&C architecture for a Nuclear Power Plant [7]

Fig. 1 is a simplified illustration of I&C systems for controlling the plant [7]. The left side of the figure is the plant control system, which is composed of digital computers, digital data networks, automatic calculations, and microprocessor-based sensors. The right side of the figure is the plant protection system, which is based on analog technology. The figure also illustrates the features of independence, redundancy, and diversity that are essential in the design of I&C systems.

2. Common Cause Failure (CCF)

Nuclear regulatory bodies have recognized CCFs as a critical weakness in redundant component implementations of nuclear control systems [8].CCF defined as the failure of a number of devices or components to perform their functions as a result of a single specific event or cause. Such failures may affect a number of different items important to safety simultaneously. This event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human induced event or an unintended cascading effect from any other operation or failure within the plant. CCF may also occur when a number of the same type of components fail at the same time. This may be due to reasons such as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency. To minimize the effects of CCF, redundancy, diversity and independence, are used asfar as practicable in the design.As shown in Fig. 2, CCF can occur only when two factors are presented concurrently [9]:

1- A latent systematic fault exists, and
2- A corresponding triggering mechanism is activated by a signal trajectory.

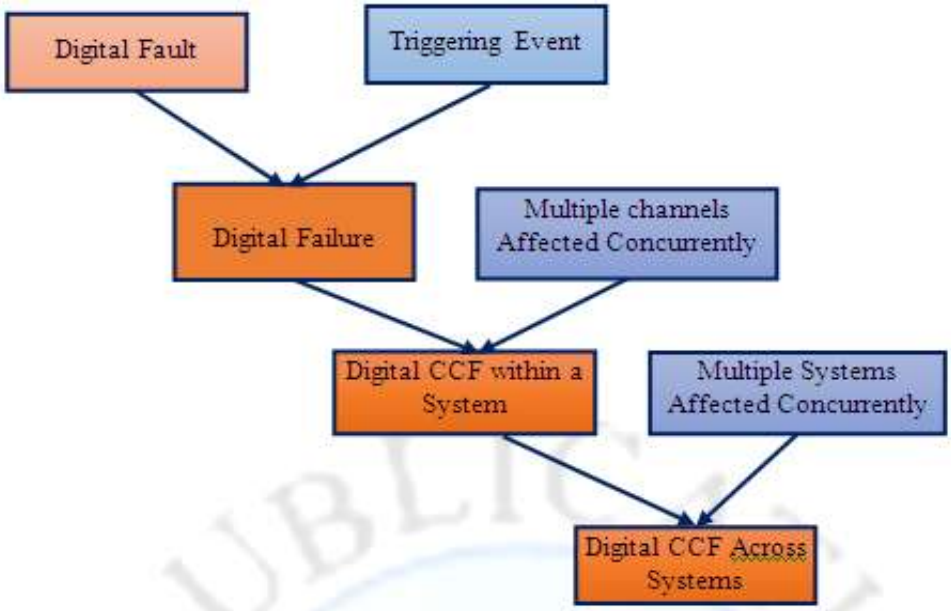

Fig. 2. Conditions of Common Cause Failure in Digital Instrumentation and Control System

2.1. Common Cause Failure Defense

The use of microprocessors and computers is not new in nuclear power plants. Early applications were limited to programmable logic controllers and plant process monitoring computers. In the 1980s, digital technologies were integrated into control systems for various subsystems, starting with the auxiliary systems and then moving to primary systems. By the 1990s, microprocessors were being used for data logging, control, and display of many non-safety-related functions [10].
To ensure reliability of safety systems based in digital I&C, diversity and defense-in-depth techniques are used in the design of digital I&C systems. Diversity is proposed as a solution for CCF problem in redundant systems. Defense-in-depth is an important term connected with nuclear safety and recommend by the IAEA in the prevention and mitigation of unsafe conditions [11].There are three complementary ways to prevent CCF, all of which contribute to defense-in-depth. They are diversity, redundancy and independence.

Diversity is usedto achieve the required levels of safety and reliability, the system should be designed based on multiple diverse components performing the same or similar functions [12]. For a particular function, two or more redundant systems or components with different attributes are included in the design. This could be achieved by using different components based on different designs and principles, from different vendors. Redundancy means that alternative systems and components performing the same function are included in the design, so that anyone can perform the required function if the others fail.

To ensure that a safety system conforms to the single failure criterion and achieve the reliability goals, the principle of redundancy shall be applied. Redundancy means provision of alternative (identical or diverse) elements or systems so that anyone can perform the required function regardless of the state of operation or failure of any other. It is typical that a safety system consists of many independent channels, which provides the same function. If a single failure occurs, their effect is limited to one channel and the failure cannot penetrate to the others. But, it is necessary to point out the requirement of redundant channels' independence. On the one hand, redundancy increases the reliability of safety actions, but on the other hand, it increases the probability of a spurious operation. The coincidence of redundant equipment signals is therefore used to obtain a proper balance of reliability and freedom from spurious operation [13].

Independence is intended to prevent the propagation of failures and CCFs due to common internal plant hazards.Digital instrumentation and control systems in nuclear power plants employ independent protection systems to detect system failures in order to isolate and shutdown failed subsystems [12]. Generally, the reliability of systems can be improved by maintaining the following features for independence in design [9]:

- Independence among redundant system components;

- Independence between system components and the effects ofpostulated initiating events PIEs such that, for example, a PIE does not cause the failure or loss of a safety system or safety function that is necessary to mitigate the consequences of that event [6];
- Appropriate independence between or among systems or components of different safety classes; and
- Independence between items important to safety and those not important to safety. For I&C independence is achieved by electrical isolation, physical separation and independence of communications between systems [13].

3. Diversity Attributes

The principle of diversity can be used to cope with potential failures, e.g. certain CCFs or uncertainties in the design or design analysis. Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event [14]. Diversity plays a very important role in case of computer-based instrumentation and controls systems. Because of uncertainties of hardware (e.g. hidden errors in microprocessors) and software (e.g. hidden errors in software development phase, in compilers, in linkers and libraries), there is a requirement to diverse these protection systems. As an example the safety system of the NPP Temelín [15] can be mentioned, where in this system there are two different protection systems, primary and secondary. The primary protection system is based on the Intel X86 microprocessors and programming in the C language, while the diverse secondary protection system utilizes the Motorola 68k microprocessors and the ADA programming language. Diversity principal is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when it is needed. Defenses at different levels of depth may also be diverse from each other. There are six important types of diversity to consider, human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity [16]:

1- Human diversity, the effect of human beings on the design, development, installation, operation, and maintenance of safety systems is known to be extremely variable, and has been a factor in several serious accidents.
2- Design diversity is the use of different approaches, including both software and hardware, to solve the same or similar problem.
3- Software diversity is the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goal.
4- Functional diversity, two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects.
5- Signal diversity, is the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.
6- Equipment diversity is the use of different equipment to perform similar safety functions, in which "different" means sufficiently unlike as to significantly decrease vulnerability to common failure.

4. I&C Defense-in-depth and diversity

There are three levels of Defense-in-depth and diversity used innuclear power plants design. The first level is at the plant functional level, by the provision of more than one function to accomplish independently a defined safety function. The second level is at the I&C systems architecture level, by a structure of a number of independent systems that can perform redundant or diverse functions. The third level is at the system level, by structuring each system into a number of independent subsystems and channels that can perform redundant or diverse functions [17].

The levels or barriers of defense-in-depth principle to the arrangement of I&Cs are the control system, the reactor trip or scram system, the Engineered Safety Features actuation system (ESFAS), and the monitoring and indicator system. The levels may be considered to be concentrically arranged as shown in Fig.3 in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity [18]. All four levels depend upon sensors to determine when to perform their functions, and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences [18, 19, 20].

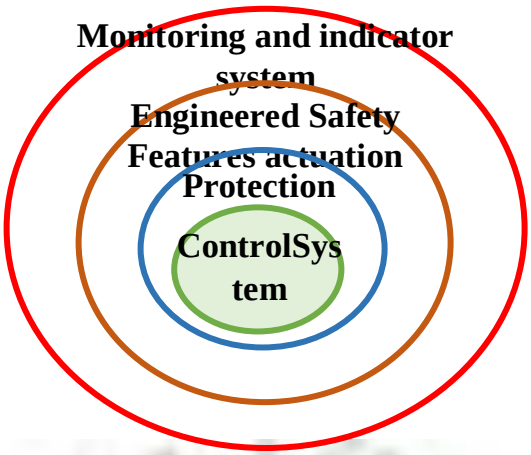

Fig.3 I&C defense-in-depth

Proposed I&Cs Defense-in-Depth Diversity

In this paper, we propose four levels for defense-in-depth and diversity for I&Cs. One level is added to the above-mentioned three levels, plant functional level, I&Cs architecture level, and subsystems level as shown in Fig.4. The fourth level will be the level of processing which is based on software and hardware by providing redundancy and diversity in both components. Processing level represents the core level and the most important level compared to other higher level. It is similar to fuel cladding in the general defense-in-depth used in safety design basis in nuclear power plants.

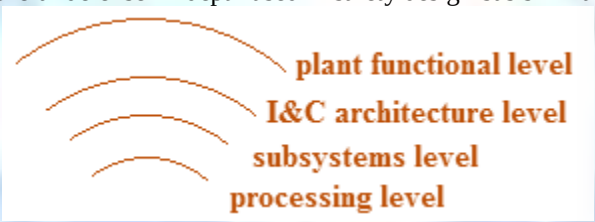

Fig. 4: Proposed four level Defense-in-Depth Diversity in digital I&Cs

More intention should be given to processing software development requirements in designing I&C systems to minimize software latent faults, which make the system vulnerable to CCF and cyber-attacks. The functional success of higher level of I&C systems essentially depends on the accuracy and quality of the underlying processing software and hardware. Consequently the reliability of digital I&C systems and its associated subsystem depends on the reliability of processing software and hardware. In digital I&C systems, processing software and hardware is an intermediate level between sensors, which provide plant status, and other levels of protection, monitoring, supervision, and actuation. The contribution of this paper is to enhancing reliability of digital I&Cs, by diversity beside redundancy, and separation means, which shall be provided at the processing level to fulfill the assigned safety functions successfully.

4.1. Hardware diversity

The diversity usage classification scheme involves three families of strategies [21,22]: (1) different technologies, (2) different approaches within the same technology, and (3) different architectures within the same technology. Using this convention, the first diversity usage family, designated Strategy A, is characterized by fundamentally diverse technologies. Strategy A at the system or platform level is illustrated by the example of analog and digital implementations. The second diversity usage family, designated Strategy B, is achieved through the use of distinctly different technologies. Strategy B can be described in terms of different digital technologies, such as the distinct approaches represented by general-purpose microprocessors and field-programmable gate arrays. The third diversity usage family, designated Strategy C, involves the use of variations within a technology. An example of Strategy C involves different digital architectures within the same technology, such as that provided by different microprocessors (e.g., Pentium and Power PC). The grouping of diversity criteria combinations according to Strategies A, B, and C establishes baseline diversity usage and facilitates a systematic organization of strategic approaches for coping with CCF vulnerabilities. Effectively, these baseline sets of diversity criteria constitute appropriate CCF mitigating strategies for digital safety systems.

4.2. Software diversity

Many requirements are developed to reduce the possibility that assumed latent software faults that may triggered from data which depend on transients of the plant process [22]. The essential idea of diverse software is to develop dissimilar software versions by employing different processes such as different software engineering practices and procedure [23]. This leads to negative covariance between dissimilar versions failures i.e. achieving failure diversity with respect to design faults that induce failures. The following features of diversity can contribute to achieving the goal of failure independence of software-based systems and resolving software CCF:

1- Software diversity features (e.g. functional diversity, different design specifications, and different functional implementation).
2- Diversity at the system level (e.g. independent diverse actuation system, different basic technology, different types of computers, hardware modules and major design concepts, and different classes of computers).
3- Diverse design approaches (e.g. algorithms, system data, hardware for inputs or interfaces, timing and sequencing).
4- Different design and implementation methods (e.g. languages, compliers, support libraries, software tools, programming techniques, system and application software, software structures, and data).
5- Diverse testing.
6- Diverse management approaches (separation of design teams, forced diversity between design teams, restricted communication between teams, and different staff).

5. Improving reliability of I&C systems

Based on the consensus practices introduced in many international standards such as IEC61513, IEC 62340, and IEC60880, for coping with CCF vulnerability in digital I&C systems, we introduce enhanced and more reliable I&C architecture based on defense-in-depth and diversity, redundancy, and independence as shown in Fig. 5. In this architecture, there are two redundant and fully diverse reactor protection systems RPSs, primary RPS and secondary RPS which are based on 2 out-of 4 redundant and diverse input channels. These two systems are designed according to the following requirements [24]:

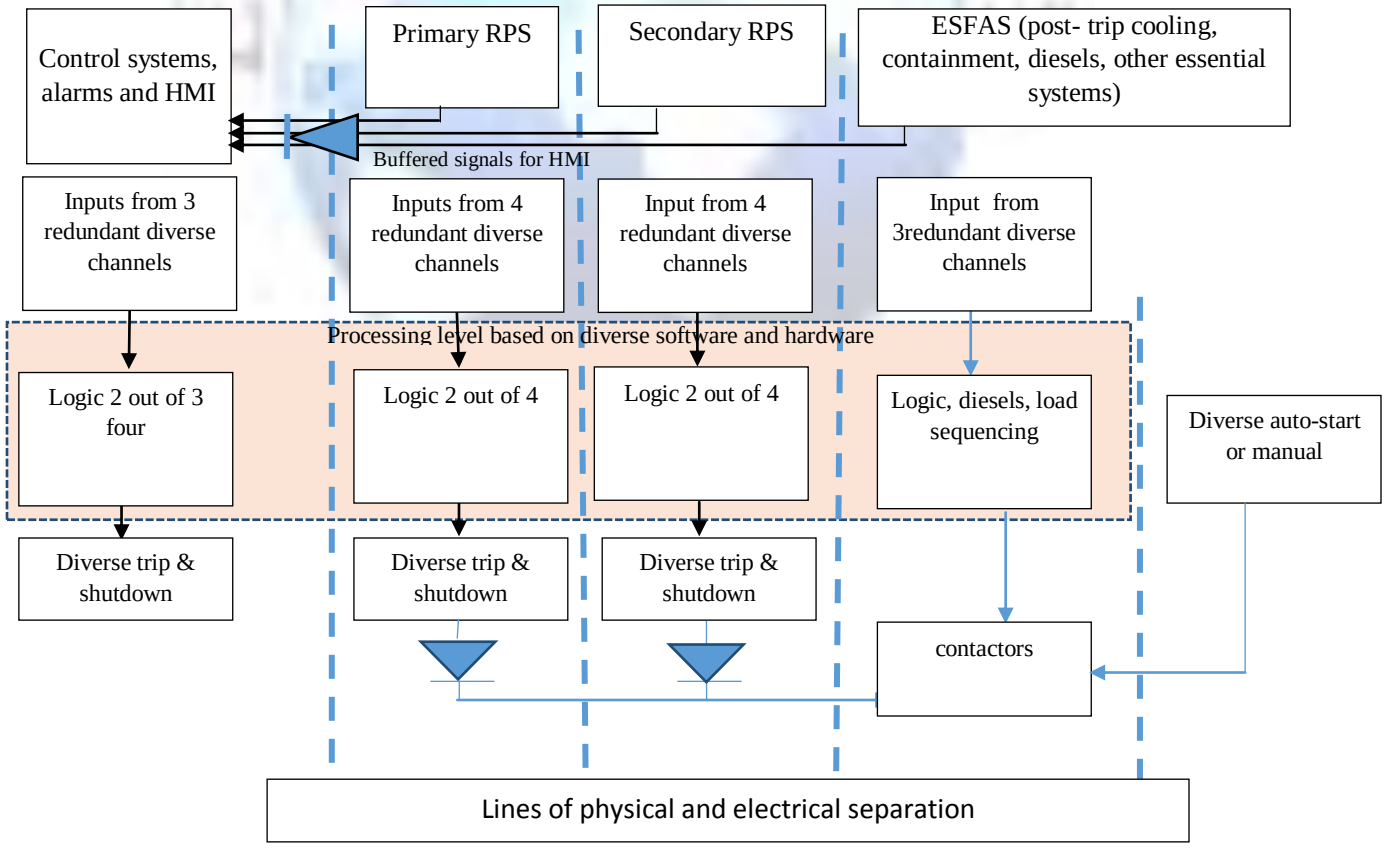

Fig.5, Improved I&Cs Architecture (Adapted from [24])

- The redundant RPSs design should be developed by a different team, using independently derived safety functional requirements;
- The redundant RPSs should be electrically and physically separated;
- They should use different input sensors measuring diverse operating parameters;
- Their signals should pass via separate routes and be processed by diverse processing logic.
- Their final actuating devices should be from a different manufacturer;
- Their means of shutdown should use different physical principles (e.g. boron injection vs. control rods).

Engineered Safety Features Actuation System (ESFAS), this is the post-trip protection system, which actuates a variety of functions after a reactor shutdown. The system objectives will be successful post-trip reactor cooling, and ensuring containment integrity. Its functions may include (depending on the NPP design) start-up of essential diesel generators, timed sequencing of loading up the generator loads, post-trip feedwater supply to steam generators, reactor coolant pumps, containment systems, etc. The design requirements of ESFAS are:

- The system shall be physically and electrically separated.
- The system shall be based on redundant2 out-of 3 diverse input signals.
- The system shall be based on diverse processing logic (software and hardware).
- The system shall use diverse actuation devices

The control system and human machine interface HMI is based on three redundant input channels and 2 out-of 3 processing logic. The HMI encompasses displays, alarms and manual controls also, indicating the status of post-trip cooling and containment systems. The design requirements for the control system are:

- Control system shall be physically and electrically separated.
- Control system shall be based on redundant and diverse signals
- According to the data processing of control system and HMI, diverse processing logic (software and hardware) shall be used.

By taking into account the considerations of diverse logic processing of input signal beside other types of diversity, the whole system reliability will be enhanced. This claim is based on the fact that, diverse logic processing is complementary to signal diversity, which enables the achievement of other diversity attributes such as functional diversity. Signal diversity and functional diversity will augment the defense of CCF through diversification of execution profile, diverse platform, and different responses to external influences. Therefore, the expected impact is to reduce the systematic faults being introduced throughout the I&Cs lifecycle process by decreasing the likelihood of CCF. The expected Probability of Failure on Demand PFD for both RPS and ESFAS will be more than $10^{-4}$and for control and monitoring system will be more than10^{-2} as compared to the proposed design in [24] which, is based on limited usage of diversity and has expected PFD in the range $10^{-3}$to 10^{-4} for PRS and ESFAS, and 10^{-2}PFD for control and monitoring system.

Conclusion

This paper discussed enhancing the reliability of digital I&Cs by defensing CCF which represents the main defect of digital I&Cs. The paper proposed extending the approach of defense-in-depth and diversity to new level. This level is the processing logic level, which is based on digital technology. Diversifying this level represents a remedy to latent software faults and hardware design or implementation faults which lead to CCF in digital I&Cs. Diversifying processing logic is a complementary and necessary attribute to realize other diversity attributes in addition to redundancy and independence. Finally, in this paper a fully diversified digital I&Cs architecture is proposed. This architecture is based two redundant and fully diversified RPSs. The processing logic of these two systems are 2out-of4. The control and monitoring system is based on 2out-of 3 redundancy and diverse processing logic. Also, the ESFAS is based on 2 out-of 3 redundant and diverse channels and diverse processing logic. The processing logic in PRSs, control and monitoring, and ESFAS is based on fully diverse software and hardware. Compared to other I&Cs architectures which use redundant RPSs, one is hard-wired and the other is software based system, it is expected that proposed architecture will be more reliable. In addition, the reliability of ESFAS and control system will be more reliable since they are based on diverse processing logic.

References

[1]. Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments. US Nuclear Regulatory Commission, 2006.
[2]. IAEA TECDOC 1016 – Modernization of instrumentation and control in nuclearpower plants, IAEA Austria, Vienna 1998.
[3]. IAEA NP-T-1.4 - Implementing digital instrumentation and control systems in the modernization of nuclear power plants, IAEA Austria,Vienna 2009.
[4]. IAEA TECDOC 1066 - Specification of requirements for upgrades using digitalinstrument and control systems, IAEA Austria, Vienna 1999.
[5]. IAEA TECDOC 1389 – Managing modernization of nuclear power plantinstrumentation and control systems, IAEA Austria, Vienna 2004.
[6]. GLÖCKLER Oszvald, "Importance of modern instrumentation and control systems in nuclear power plants," Nuclear Safety and Simulation, Vol. 4, Number 4, December 2013.
[7]. US National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues), 1997.
[8]. Wood, Richard Thomas, et al. Diversity strategies for nuclear power plant instrumentation and control systems. No. ORNL/TM-2009/302. Oak Ridge National Laboratory (ORNL), 2010.
[9]. IAEA SSR-2/1Safety of Nuclear Power Plants: Design, Austria, Vienna, 2012.
[10]. US National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues), 1997.
[11]. Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-in-Depth Strategies, Homeland Security, October 2009.
[12]. Voas J, Ghosh A, Charron F, "Reducing Uncertainty about Common-Mode Failures," the Eighth International Symposium on Software Reliability Engineering, 1997, 308-319.
[13]. IAEA NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Austria, Vienna, 2002.
[14]. IAEA NP-T-1.5, Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, Austria, Vienna, 2009.
[15]. Siu, Nathan, et al. Use and development of probabilistic safety assessment-CSNI WGRISK. Organisation for Economic Co-Operation and Development, Nuclear Energy Agency-OECD/NEA, Committee on the safety of nuclear installations-CSNI, Le Seine Saint-Germain, 12 boulevard des Iles, F-92130 Issy-les-Moulineaux (France), 2007.
[16]. Preckshot, G. G. Method for performing diversity and defense-in-depth analyses of reactor protection systems. Nuclear Regulatory Commission, Washington, DC (United States). Div. of Reactor Controls and Human Factors, 1994.
[17]. Kharchenko, Vyacheslav, et al. "Fault Insertion Testing of FPGA-Based NPP I&C Systems: SIL Certification Issues." 2014 22nd International Conference on Nuclear Engineering. American Society of Mechanical Engineers, 2014.
[18]. Huang, H.-W., Shih, C., Yih, S. and Chen, M.-H. (2008). System-level hazard analysis using thesequence-tree method. Annals of Nuclear Energy 35, pp. 353–362.
[19]. A. Z. Mesquita, A. C. L. Costa, and R. M. G. P. Souza, "Modernization of the CDTN IPR-R1 TRIGA reactor instrumentation and control," in Proc. International Nuclear Atlantic Conference (INAC 09), October 2009.
[20]. NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.U.S. Nuclear Regulatory Commission, Washington D.C., 20555-0001, 1994.
[21]. Wood, Richard Thomas, et al. Diversity strategies for nuclear power plant instrumentation and control systems. No. ORNL/TM-2009/302. Oak Ridge National Laboratory (ORNL), 2010.
[22]. U.S. Nuclear Regulatory Commission, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG/CR-7007, ORNL/TM-2009/302, Washington, D.C., 2010.
[23]. Benoit Baudry and Martin Monperrus. The multiple facets of software diversity: Recent developments in year 2000 and beyond. CoRR, abs/1409.7324, 2014.
[24]. Jim Thomson, Nuclear Power Station Control and Instrumentation Safety Systems. Architecture - An Overview. March 2012 v. 2.1, Available at:http://www.safetyinengineering.com/FileUploads/nuclear%20C&I%20architecture%20v2_1330947816_2.pdf