Application of Reliability Analysis in Preliminary Design Stage of Digital I&C System

Wenjie Qin[a*], Xuhong He[b], Xiufeng Tian[c], Dejun Du[c]
[a]Lloyd's Register Consulting – Energy Inc., Shanghai, China
[b]Lloyd's Register Consulting AB, Stockholm, Sweden
[c]China Nuclear Power Engineering Co., Ltd., Beijing, China

Abstract: In the engineering process of a new build nuclear power plant, reliability analysis of the digital I&C systems is often performed at a later engineering stage based on detailed I&C design. However, the reliability analysis performed in such stage is generally too late in the engineering cycle to correct any essential design issue in an easy way and would provide very limited possibility to the I&C designer to implement design changes in case the reliability requirement is not achieved.

This paper presents the application of the reliability analysis in the preliminary design stage of the digital I&C system in a Chinese new build nuclear power plant project. Analysis in early stage can provide insights in various fields, such as: preliminary validation of I&C reliability requirements in order to avoid fundamental design issues, I&C architecture improvement, recommendation on I&C signal allocation, module level and system level self-test design, periodic test coverage and interval, maintainability requirement, and even on the fluid system design etc. The objective of the study is to ensure the fulfillment of I&C reliability requirement with the final I&C design and provide early stage improvement recommendations for the I&C design.

Keywords: Digital I&C, Reliability analysis, Preliminary design stage

1. INTRODUCTION

Digital Instrument & Control (I&C) systems are commonly used in new nuclear power plants. As the digital I&C systems play a critical role in plant safety and availability, there is a need to quantitatively assess the reliability of such systems.

The reliability analysis of digital I&C systems are often performed in two contexts:

- To validate the fulfillment of reliability and availability requirements. Such requirements are generally specified in the contract of the plant owner.
- Or, in Probabilistic Safety Assessment (PSA) for the modeling of I&C systems. I&C systems are modeled either as support systems to mitigation functions (e.g. failure of safety I&C signal in case of accident), or as part of the initiating event (e.g. spurious signal actuation).

A typical I&C development process is given in Figure 1 (Ref. [1]). Generally, the reliability analysis mentioned above is performed after hardware and software implementation stage, when the detailed I&C design is finalized. The objective of such analysis is more to evaluate the reliability level as it is than to provide insights or recommendations to the I&C designer. The main reason is that after finalization of detailed I&C design, it is very costly to make significant design change of the I&C systems, especially change on hardware and system architecture.

[*] wenjie.qin@lr.org

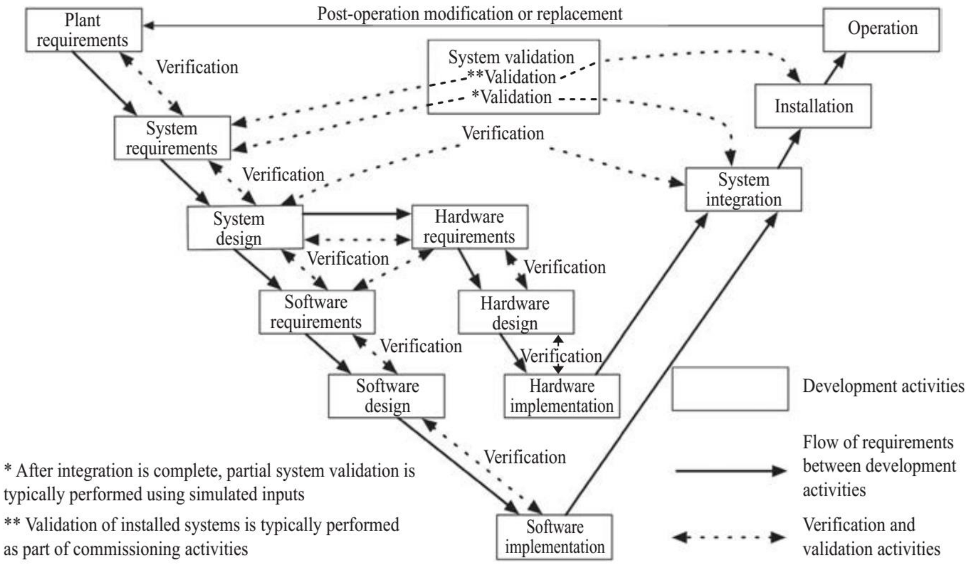

Figure 1: Typical I&C development lifecycle processes and V&V activities

As the reliability analysis of I&C systems can provide valuable insights to the designer, to perform such analysis in early I&C design stage (i.e. beginning of hardware and software design in Figure 1) when design changes can still be easily incorporated, is beneficial in the aspects such as:

- To guarantee the fulfillment of the reliability objective, reduce the risk of non-conformity and late stage design change
- To provide insights, recommendations and requirements to the I&C and system designers to improve the overall design
- To optimize the maintainability of the I&C systems

This paper presents the application of the reliability analysis in the preliminary design stage of a digital I&C system in a Chinese new build nuclear power plant project. The discussion focuses on the specificities of the analysis method and the useful insights that the analysis has provided.

2. Analysis method and specificities

2.1. General analysis method

Digital I&C systems include unique features, such as dynamic interactions, usage of software and internal state transitions, to perform reliability analysis on such systems, a number of modeling methods have been tested and discussed. There are mainly 2 types of methods: the traditional Fault Tree Analysis (FTA) method and the dynamic reliability methods. A summary of experiences of modelling digital systems in CSNI member countries can be found in Ref. [2].

Generally, dynamic methods provide a more accurate representation of probabilistic system evolution in time than the FTA method. There exists several dynamic reliability approaches, and Dynamic Flowgraph Methodology (DFM) and Markov/CCMT (Cell-to-Cell Mapping Technique) are ranked as the two top dynamic reliability modelling approaches with the most positive features and least negative features (Ref. [3]). However, the dynamic methods are on a trial stage, there is not yet enough industrial experience available for the analysists. In addition, such methods require large amount of knowledge and detailed input data of the system being studies, which are not available in the preliminary design stage.

The analysis in this case is applied on reactor protection system which does not have control loop, the FTA mothed is considered sufficient according to the position of experts discussed in Ref. [2]. In addition, the analysts having PSA experiences are familiar with the FTA method. Therefore, the FTA method has been chosen for this application.

A typical reliability analysis is performed with the following steps:

i. Definition of working scope

The working scope means which I&C systems and functions are included in the reliability study and what are the interested analysis cases to be considered. The working scope depends on the purpose of the analysis. For example, to validate the reliability level of an I&C system, the analysis shall cover in an exhaustive way all functions implemented in the system, however, for a reliability analysis regarding I&C functions credited in PSA, only relevant functions are analyzed.

ii. Collection of input data

The input data includes items such as: functional requirements of the analyzed I&C systems and functions, I&C system functional description, fluid system description and P&IDs, I&C hardware and software description, reliability data, and operational data (such as repair time, test interval, etc.)

iii. Detailed description of the analyzed I&C system and function

In this step, aspects such as I&C system architecture, overall operation of the I&C system, hardware composition of the chosen function, self-monitoring and periodic test concept, are described in detail.

iv. Failure Modes and Effects Analysis (FMEA)

The FMEA covers all failure modes of all modules involved in the chosen I&C function. This step helps the reliability analyst to have a profound understanding on how the I&C function may fail and how failure is detected, and thus forms a solid basis for the fault tree modeling work.

v. Fault tree modeling and quantification

The fault tree modeling is the key step in the reliability analysis. In the modeling of I&C functions, the essential factors include: definition of the failure/success criteria of the I&C function, representation of the voting logic, automatic and manual reconfiguration after failure detection, consideration of Common Cause Failure (CCF). A structural modeling approach is beneficial to lower the possibility of error, and the level of detail modeled must be consistent with the analysis purpose. Sensitivity analysis cases are created and quantified in this step.

vi. Conclusion

The conclusion contains quantification results and most importantly the insights based on these results.

2.2. Specificities for reliability analysis in preliminary I&C design stage

To perform the reliability analysis in preliminary I&C design stage, a number of aspects differentiate from the regular reliability analysis performed with a finalized design. The following paragraphs present these specificities.

a. Working scope

As the reliability analysis in preliminary I&C design stage is performed to provide useful insights to support the design, it is not useful to cover the whole system, only representative functions should be analyzed. And for the selected systems and functions, a number of interested parameters (such as architecture, reliability data, test interval, etc.) can be analyzed through sensitivity cases. The definition of working scope shall be determined by the reliability analyst together with the I&C designer and the involvement of process/safety and fluid system designers.

b. Input data

It is obvious that the main difficulty of performing reliability analysis in preliminary I&C design stage is the shortage of input data. Another difficulty is that the input data may evolve quickly in such stage. Following measures can be used to overcome these difficulties:

- Keep close connection with I&C designer. As the input data are not complete and the preliminary documentation can probably not reflect the latest status of the I&C design, it is crucial to involve deeply the I&C designer in the reliability analysis. Ideally, the reliability analysis is performed with a team composed with I&C designer and reliability analyst.
- Use of generic database. In preliminary I&C design stage, the I&C platform is normally already chosen, the specific reliability data can then be used. However, for equipment such as sensor and relay, it is likely that the product is still unknown. Therefore, data in generic reliability database such as Ref. [4] should be used, and if it turns out that these data have significant impact on results and conclusions, sensitivity analysis shall be made to define reliability requirement on them.
- Make reasonable assumption. For parameters which are not available in generic reliability database (e.g. test interval, self-test coverage rate of certain components), assumption should be made after discussion with relevant specialists. For hardware/software configuration which is not available, typical configuration or the most probable configuration should be assumed after confirmation by I&C designer. All assumptions shall be well documented, and if the results show that the assumed parameters have significant impact on results, sensitivity analysis shall be done to obtain recommendations or requirements on them.
- Limit the scope of analysis. If the reliability analysis in preliminary stage is to provide insights to the I&C hardware design, factors such as human error can be excluded from analysis. Actually, to evaluate human error, especially errors made in maintenance activities, documents produced in a later design stage are necessary.

c. Fault tree modeling

As a common practice, the fault tree modeling of I&C function starts from the I&C output signals and includes all failure modes of all relevant components leading to the failure of these signals. This modeling is repeated level by level until all components are represented in the failure trees. According to the analysis purpose, different levels of details may be used in the modeling, such as I&C unit level, I&C module level and basic component level.

The fault tree modeling of reliability analysis in preliminary I&C design stage follows the same approach, nevertheless, to obtain sufficient level of details in the insights and to facilitate the performance of large number of sensitivity analysis cases (especially those on I&C architecture), the modeling shall consider the following recommendations:

- The modeling at I&C module level is appropriate in most cases. The modeling at unit level can be in some cases sufficient if the objective is to validate the overall I&C architecture or the system level redundancy, however, such modeling can not provide detailed insights to the I&C designer.
- The modeling of the architectural elements such as I&C units, sub-systems and networks should be separable to allow easy implementation of sensitivity cases. For example, for a voting unit receives signals from 2 redundant acquisition units, the failure of 2 input signals to

the voting units should be modeled in 2 different fault trees, so that one can easily create different sensitivity cases to evaluate the impact of removing or adding redundant signal.

d. Participants to the analysis

Generally, I&C reliability analysis requires the participation of reliability analyst and I&C designer. I&C designer helps the reliability analyst to better understand the composition, operation and failure mode of the I&C system, and sometimes participates directly to the work such as FMEA.

For the reliability analysis in preliminary I&C design stage, in addition to the I&C designer, it is indispensable to involve the process/safety designer and fluid system designer. The reason is that, in most of cases, the I&C function is specified by the process/safety designer or by the system designer, it is essential to understand the role of the analyzed I&C function in the safety of the plant and then operation of the fluid systems. As the documentation is not complete in preliminary design stage, these upstream teams shall be involved in the beginning of the reliability study in order to clarify the definition of I&C function scope and the success criteria.

3. Application case

The reliability analysis is performed in the preliminary design stage of the Reactor Protection System (RPS) in a Chinese new build nuclear power plant project. The main safety functions implemented in the system are automatic Reactor Trip (RT) functions and automatic Engineering Safety Feature (ESF) actuation functions. The analysis performed focuses on the typical automatic ESF actuation functions, such as the automatic actuation of safety injection.

The preliminary RPS architecture of automatic ESF actuation function is presented in Figure 2. The I&C system is divided into tow sub-systems (denoted by X and Y) with the same architecture, so as to ensure the separation of certain I&C functions which are functionally diversified. The sensors and signal acquisition/calculation (by Acquisition Unit) are implemented in 4 redundant divisions. The logic signals generated in AU are then processed in Voting Units (VU) with 2-out-of-4 voting logic. Signals generated in VU of the 2 sub-systems are combined with a hardwired "AND" logic before being sent to Priority Controller (PC) of each actuator.

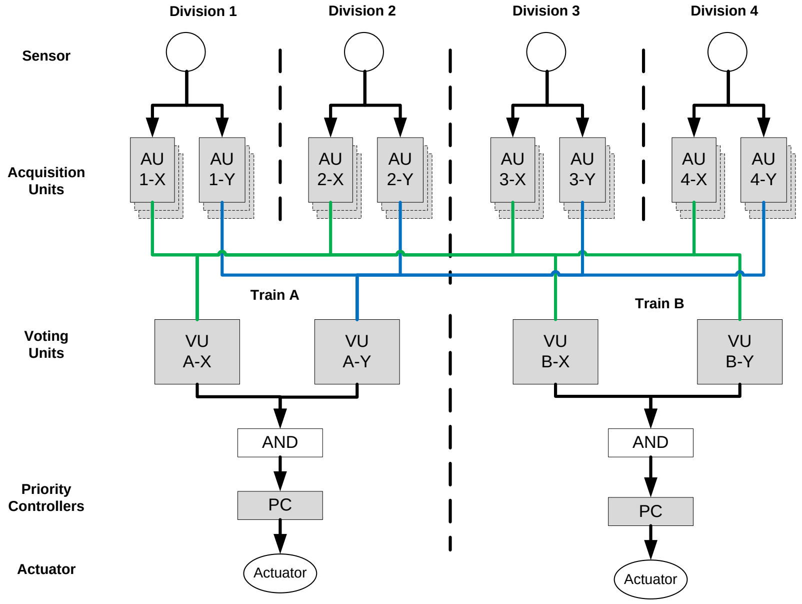

Figure 2: Preliminary I&C architecture of automatic ESF actuation function

4. Useful insights

In addition to the baseline model, a large number of sensitivity cases are analyzed in the application, providing useful insights. Some of the insights are presented in the following paragraphs.

4.1. Definition of success criterion in accident mitigation

One of the typical functions analyzed is the automatic actuation of safety injection. The preliminary safety injection system layout is presented in Figure 3. The safety injection system is composed of 2 trains (A and B), in each of the train, there is a High Pressure (HP) injection circuit and a Low Pressure (LP) injection circuit. According to the discussion with process and safety designers, in accident analysis, the combination of one HP injection and one LP injection is sufficient to mitigate the accidental sequences. However, it is not yet clear in this stage if the combination shall be in the same train or can be between different trains.

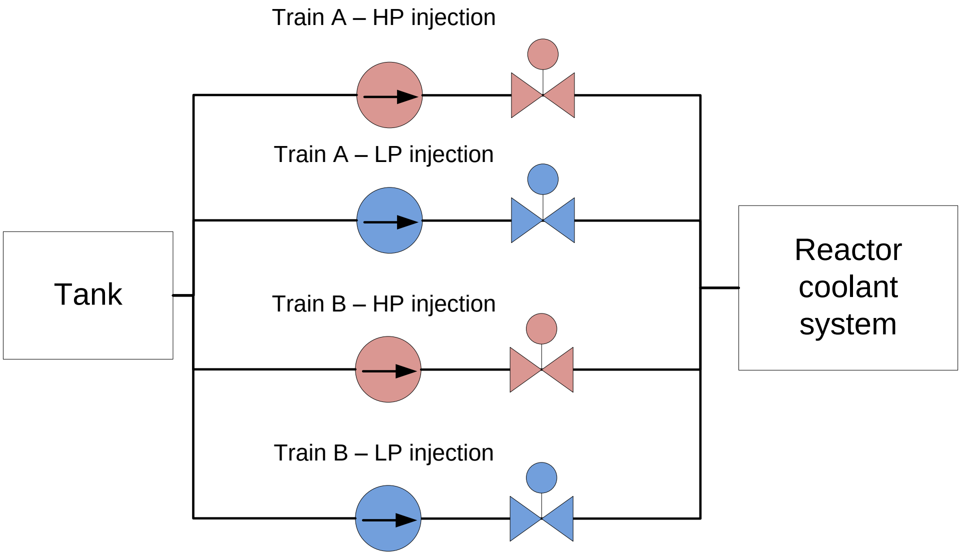

Figure 3: Sketch of safety injection circuits

Sensitivity cases are created to evaluate reliability impact with different success criteria:

- Case 1A: success criterion = (one HP injection in Train A OR B) AND (one LP injection in Train A OR B)
- Case 1B: success criterion = (one HP injection AND one LP injection in Train A) OR (one HP injection AND one LP injection in Train B)

The results show that comparing to the case 1A, the probability of failure per demand (PFD) with success criterion of case 1B has an increase of 68%.

Therefore, it is recommended to ensure the validation of success criterion of case 1A in accident analysis, and implement if necessary design measures in safety inject system so that such “inter-train” combination of HP and LP injection is equivalent to the “inner-train” combination.

4.2. Fluid system line-up

According to the discussion with system designers, the Motor-Operated Valves (MOV) downstream the injection pumps in Figure 3 are closed during normal operation and need to be opened in case of safety injection actuation. However, it is possible to credit the check valves downstream the MOV to ensure the isolation from reactor coolant system during normal operation and keep the MOV open. In such case, the failure of MOV opening (both I&C signal failure and mechanical failure) will not impair the effectiveness of safety injection function.

Sensitivity cases are created to compare the following line-up configurations in terms of I&C reliability:

- Case 2A: MOV closed during normal operation and need to be opened in case of safety injection actuation
- Case 2B: MOV open during normal operation

The result shows that comparing to case 2A, the PFD with line-up configuration in case 2B has a decrease of 53%. And in considering the mechanical failure risk, the decrease will be even higher.

Therefore, it is recommended to implement measures in safety injection system design and operating/maintenance instructions to ensure the open position of MOV during normal operation.

4.3. I&C function allocation

As shown in Figure 2, there are 2 sub-systems in the RPS. Some I&C functions (such as 2 RT functions for the same initiating event) are implemented in different sub-systems to ensure the separation of functions which are functionally diversified, but for other I&C functions, no requirement is expressed by the upstream team, and the I&C designer has then the possibility to choose the allocation in one or both sub-systems.

Sensitivity cases are created to compare the following allocation choices:

- Case 3A: Automatic ESF actuation function implemented in both sub-systems
- Case 3B: Automatic ESF actuation function implemented in one sub-system

The result of a typical I&C function shows that comparing to case 3A, the PFD with allocation choice in case 3B has a significant increase of 201%. Although the result of case 3B still meets the reliability objective, the implementation in both sub-systems shows large improvement of reliability level.

As it is impossible to implement all functions in both sub-systems due to the I&C sizing limit, it is recommended to identify critical I&C functions by PSA, and implement when it is applicable such functions in both sub-systems.

4.4. Diversification requirement

In primary design, it is known that the components used in redundant AU and VU are the same I&C modules, therefore, the risk of Common Cause Failure (CCF) of redundant I&C modules shall be taken into account. However, it is not yet clear for some modules such as Priority Controllers (PC) if diversification is needed.

Sensitivity cases are created to compare the following diversification set-up at PC level:

- Case 4A: PC in Train A diversified from the PC in Train B
- Case 4B: No Diversification of PC

The result shows that comparing to case 4A, the absence of PC diversification in case 4B leads to a significant increase of PFD of 1085%. And such result could question the fulfillment of reliability objective. The reason is that at the level of I&C output to actuators, there is no possibility to implement additional redundancy, the failure of a PC module leads directly to the non-actuation of the corresponding actuator, and the CCF of PC has the same consequence as the CCF of actuators.

Therefore, it is strongly recommended to implement diversification in PC. And if the diversification is not feasible, simple modules (e.g. electronic modules without software application) shall be used so as to lower the possibility of CCF, and detailed analysis shall be performed to evaluate the CCF mechanism and risk.

4.5. Online-test coverage factor requirement

In the failure of I&C function, the most important failure mode is usually the failure not identified by online detection, because such failure mode can only be identified by delayed detection means such as periodic test or operator monitoring, the failure can be hidden during long time. As a result, the coverage factor of the online test (probability that a failure can be detected by online test) is a key parameter in the reliability analysis. In preliminary I&C design stage, such parameter can be unavailable, assumption is thus made.

Sensitivity cases are created to evaluate the impact of coverage rate on sensor failure detection:

- Case 5A: Coverage factor at 90%
- Case 5B: Coverage factor at 50%

The result of a typical I&C function shows that comparing to case 5A, a lower coverage factor at 50% in case 5B leads to a significant PFD increase of 268%. And the sensor part becomes the overwhelming contributor in the failure probability. With a coverage factor at 90%, the contribution of the sensor part to the PFD is at a reasonable level.

Therefore, it is strongly recommended to consider 90% of coverage factor as design requirement of safety critical sensors. All failure modes of sensors and detection means shall be analyzed and evaluated in detail. If the default online detection means (e.g. range monitoring in I&C acquisition module) is not sufficient to reach such coverage factor, additional measures such as discrepancy test between I&C divisions, regular parameter monitoring by operator shall be adopted.

4.6. Periodic test design

In the preliminary design of Periodic Test (PT) of the RPS, as shown in Figure 4, 3 PT are planned with overlapping:

- PT1: Instrumentation channel test. It covers the instrumentation part from the sensor to the input channels of the AU.
- PT2: Processing channel test. This PT covers the processing part from AU input to VU output including the processing modules and the software logics.
- PT3: Actuator control channel test. This PT covers the signal output part from VU output to the PC.

Reliability calculation cases show that the most important PT is the PT3, and the least important one is the PT2. The reason is that the online-test coverage factor is much higher in the upper part of I&C architecture than that in the lower part. For example, in case of PC output channel freezing, it is difficult to implement an automatic detection means to immediately identify the failure. One has to wait until the PT3 in which the status of the channel is effectively changed by the operator. Consequently, it is beneficial from reliability perspective to reduce the test interval of PT3. However, frequent PT leads to high work load during plant operation and may introduce human error which impairs the reliability.

Therefore, it is recommended to keep as far as possible the PT interval design target (e.g. one PT per division/train per cycle), and in case the reliability objective is exceeded, one can identify other means which may be considered as equivalent PT or cover some failure modes (e.g. Periodic test of actuator using part of I&C channel). Another choice is that when decreasing the interval of PT3, one can increase the interval of PT1 or PT2 to balance the workload in plant operation.

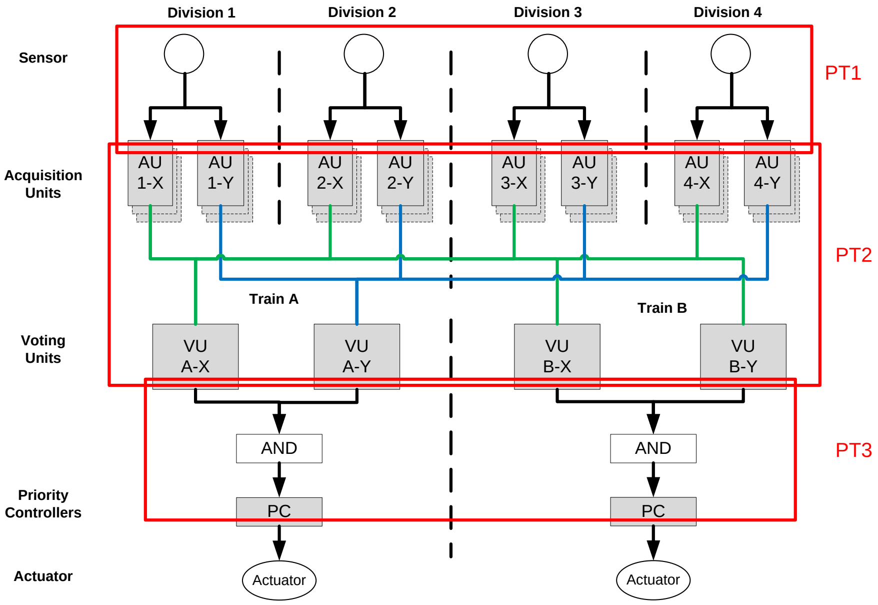

Figure 4: Scope of Periodic Tests

5. Conclusion

The previous discussion shows that it is beneficial to perform reliability analysis in the early I&C design stage. Such analysis can not only reduce the risk of non-fulfillment of reliability design objective, it can also provide useful insights to improve various design aspects.

Due to the lack of well documented data in preliminary stage, special measures should be adopted in the reliability analysis, and one of the most important one is to have deep involvement of upstream teams (such as process/safety and fluid system designers) and I&C designer in the analysis.

References

[1] IAEA Specific Safety Guide No. SSG-39 – Design of Instrumentation and Control Systems for Nuclear Power Plants

[2] NEA/CSNI/R(2009)18 - Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants

[3] NUREG CR-6985 (2009) – A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems

[4] NUREG CR-6928 (2007) - Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants