УДК 621.039.58 Doi: https://doi.org/10.32918/nrs.2020.2(86).05

Safety and Reliability Assessment of NPP Instrumentation and Control Systems Considering Different Communication Architectures

■ **Babeshko E.**
National Aerospace University «KhAI», Kharkiv, Ukraine
Research and Production Corporation «Radiy», Kropyvnytskyi, Ukraine
ORCID: https://orcid.org/0000-0002-4667-2393

■ **Illiashenko O.**
National Aerospace University «KhAI», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-4672-6400

■ **Kharchenko V.**
National Aerospace University «KhAI», Kharkiv, Ukraine
Research and Production Corporation «Radiy», Kropyvnytskyi, Ukraine
ORCID: https://orcid.org/0000-0001-5352-077X

■ **Ruchkov E.**
Research and Production Corporation «Radiy», Kropyvnytskyi, Ukraine
ORCID: https://orcid.org/0000-0002-4570-9844

Safety and reliability assessment of instrumentation and control (I&C) systems used in different safety-critical industries is a responsible and challenging task. Different assessment models recommended by international and national regulatory documents and used by experts worldwide still have disadvantages and limitations. Therefore, studies of assessment model improvements and refinements are essential. This paper proposes that the assessment models be improved by taking into account different architectures of communications both between different systems and within one particular system. In most models, communication lines are considered absolutely reliable, but the analysis performed shows that the communications should be necessarily addressed. Several analytical models are described to assess the reliability of safety-critical systems for nuclear power plants with different communication options.

Keywords: NPP I&C, safety assessment, reliability assessment, communications, probability of no-failure operation.

Safety-critical industries rely on protection systems that typically consist of a number of quite complicated subsystems responsible for solving particular tasks.

For example, in nuclear industry, reactor trip systems (RTS) rely on Neutron Flux Monitoring Systems (NFMS) to monitor neutron radiation levels within the core which can safely shutdown the reactor if levels exceed sensor set-points.

The reliability and safety analysis of such critical I&C systems does not sufficiently consider possible options of communications between subsystems of protection systems, as well as possible ways of communications within particular system are usually not addressed adequately. In this work, we summarize possible ways for interconnections between different systems and different ways of communications between parts of one system.

Safety-critical systems were initially based on the single controller architecture where no communications were needed to execute safety-related functions (Figure 1).

Wide usage of communications in safety-critical systems makes them more flexible but brings an additional safety and reliability engineering challenge due to an introduced additional 'Communications' function block [1] (Figure 2).

Moreover, in process industries it is common for a safety critical system to be one of a number of different layers of protection, each of which limits the potential for, and impact of, a hazardous event [2].

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

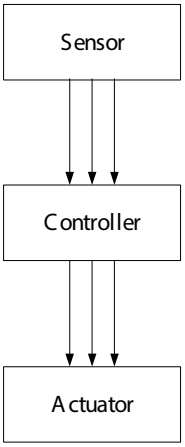

Figure 1 – Safety-Critical System without Communications

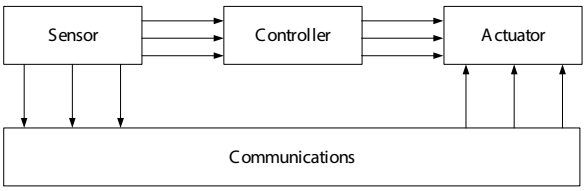

Figure 2 – Safety-Critical System with Communications

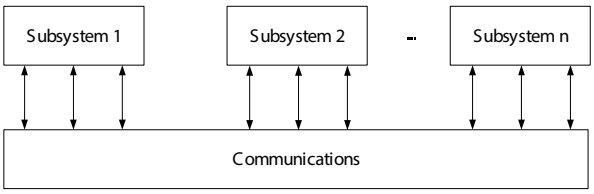

Figure 3 – Interaction of Different Subsystems via Communications

International safety standards such as IEC 61508 [3] explicitly require sufficient independence between these layers in the sense that interference between functions must not affect any safety-related function property.

In actual practices, different safety-critical, safety-related and even non-safety-related systems could share resources such as sensors, power supplies, data storage devices, cabling, etc., and, consequently, could have some communications between then (Figure 3).

Therefore, special actions need to be taken in safety and reliability analysis to ensure that a single failure does not affect both non-safety-related and safety-related systems. Similarly, if several (redundant) safety-related systems are used, it is important to consider that common cause failures should not affect both primary and secondary systems at the same time.

Recent research efforts have confirmed that the probability of overall communication failure significantly contributes to the probability of safety-related system signal failure [4, 5] and, therefore, should be addressed in reliability and safety analysis.

As for safety and reliability assessment techniques, Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD) and Markov models are of particular importance, as they are explicitly mentioned in relevant international standards like mentioned above IEC 61508.

Consideration of possible communication architectures

To demonstrate the importance of considering possible communication architectures in reliability and safety analysis, we provide analysis of a typical reactor control and protection system.

The reactor control and protection system [6] is a safety-related system responsible for:

reactor emergency protection;

fast reduction in reactor power if the main unit equipment has tripped;

unloading and limitation of reactor power if the main unit equipment has tripped;

operational control of unit power.

The system usually includes the following layers (Figure 4):

Neutron Flux Monitoring Systems (NFMS) layer – typically two sets of NFMS;

Reactor Trip Systems (RTS) and Reactor Power Control and Limitation Systems (RPCLS) layer – typically several sets of RTS and RPCLS;

Rod Control Systems (RCS) layer.

The Reactor Power Control and Limitation Systems [7] perform the following main functions:

automatic and continuous control of reactor neutron power and/or pressure in the main steam line of NPP power unit turbine;

control of reactor power at levels corresponding to the range of NPP power unit main licensing limitations, from startup through full-power operation;

fast-responding preventative protection of the reactor (runback at 40-50 % of full power within 3 to 4 seconds).

The Reactor Trip System continuously monitors the actual values of neutron flux and other process variables and generates shutdown signals in case these variables reach their setpoints.

The Rod Control System is a safety-related system responsible for [8]:

indication of all reactor control and safety rod position operation parameters and real rod positions;

performance of all rod drive control functions including trip portion (set of the rod drive power supply breakers);

uninterrupted electric power supply of rod drives in normal operation;

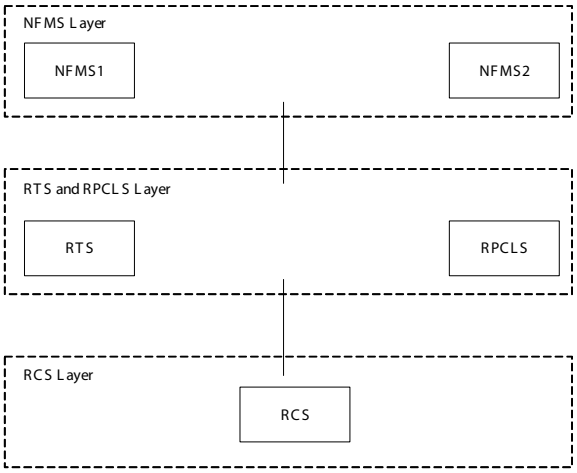

Figure 4 – Reactor Control and Protection System: Different Layers

switching off the rod drive electric power supply by emergency protection signals in case of abnormal operation that requires the reactor to be brought into a subcritical state.

With the implementation of four-channel safety system design (the «2 of 4» principle) as the most popular and commonly used approach [9], there are three main options for implementation of redundancy and communications between the different layers:

nodal «2 out of 4» majorization with one physical connection (cable) between layers and multiplication of communications at the entrances of the second layer (option A);

nodal «2 of 4» majorization with n physical connections between layers where n = {2, 3, 4} and multiplication of communication links at the outputs of the first layer (option B);

network «2 out of 4» majorization (option C).

We show these options using 'NFMS1-RTS1' interconnections as an example.

Figure 5 graphically represents the potential implementation of option A.

Figure 6 graphically represents the potential implementation of option B.

Figure 7 graphically represents the potential implementation of option C.

Using these graphical representations, it is possible to derive the expressions to calculate the probability of no-failure operation.

For option A, the expression would be the following:

$$P_A = \sum_{i=0}^{2} C_4^i P_{NFMS1-1}^{4-i}(1-P_{NFMS1-1})^i \cdot P_{2/4} \times \times P_{comm} \cdot \sum_{i=0}^{2} C_4^i P_{RTS1-1}^{4-i}(1-P_{RTS1-1}) \quad (1)$$

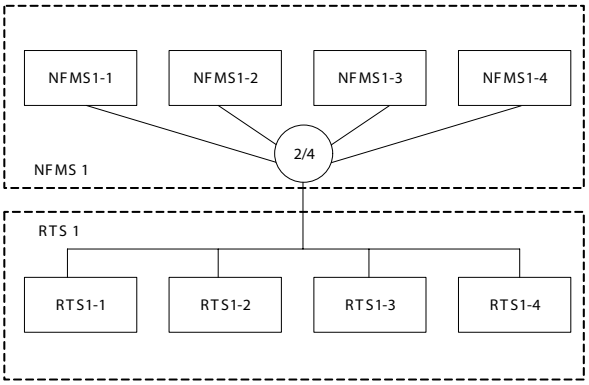

Figure 5 – Redundancy. Option A

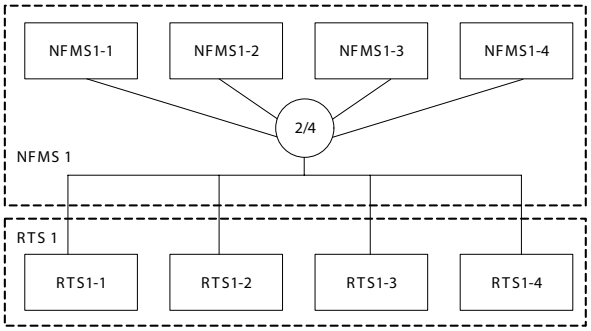

Figure 6 – Redundancy. Option B

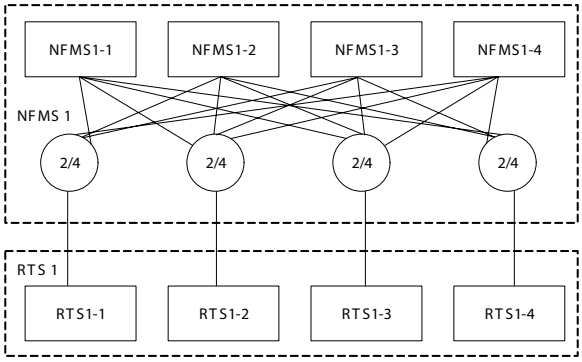

Figure 7 – Redundancy. Option C

where PA is the probability of no-failure operation of option A;

PNFMS1-1 is the probability of no-failure operation of NFMS;

P2/4 is the probability of no-failure operation of voting element;

Pcomm is the probability of no-failure operation of communications;

PRTS1-1 is the probability of no-failure operation of RTS;

C_4^i is the number of combinations.

For option B, the expression would be the following:

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

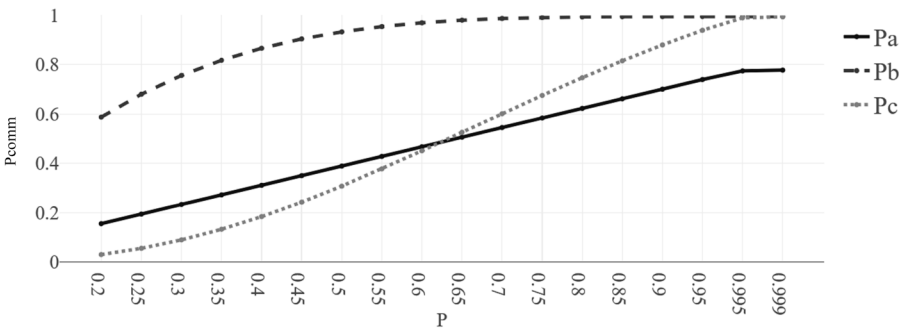

Figure 8 – Comparison of different communication architectures

$$P_B = \sum_{i=0}^{2} C_4^i P_{NFMS1-1}^{4-i}(1-P_{NFMS1-1})^i \cdot P_{2/4} \times \times[1-(1-P_{comm})^n] \cdot \sum_{i=0}^{2} C_4^i P_{RTS1-1}^{4-i}(1-P_{RTS1-1})^i \quad (2)$$

where PB is the probability of no-failure operation of option B;

PNFMS1-1 is the probability of no-failure operation of NFMS;

P2/4 is the probability of no-failure operation of voting element;

Pcomm is the probability of no-failure operation of communications;

PRTS1-1 is the probability of no-failure operation of RTS;

C_4^i is the number of combinations.

For option C, the expression would be the following:

$$P_C = \sum_{i=0}^{2} C_4^i P_{NFMS1-1}^{4-i}(1-P_{NFMS1-1})^i \times \times \sum_{i=0}^{2} C_4^i (P_{2/4} \cdot P_{comm} \cdot P_{RTS1-1})^{4-i} \times \times (1-P_{2/4} \cdot P_{comm} \cdot P_{RTS1-1})^i \quad (3)$$

where PC is the probability of no-failure operation of option C;

PNFMS1-1 is the probability of no-failure operation of NFMS;

P2/4 is the probability of no-failure operation of voting element;

Pcomm is the probability of no-failure operation of communications;

PRTS1-1 is the probability of no-failure operation of RTS;

C_4^i is the number of combinations.

Expressions (1)-(3) were obtained under the following assumptions:

NFMS channels are equally reliable (i.e. =PNFMS1-1= PNFMS1-2= PNFMS1-3= PNFMS1-4);

RTS channels are equally reliable (i.e. PRTS1-1= =PRTS1-2= PRTS1-3= PRTS1-4);

reliability of voting element is taken into account;

communications within the same system (NFMS, RTS) are absolutely reliable, i.e. only the unreliability of the communications between different systems is taken into account;

failures of the elements are independent.

The proposed options were compared using different values of Pcomm.

The received expressions could be used to obtain the reliability indices (and also safety indicators after additional processing) for the part of the reactor control and protection system and, therefore, could be utilized only for preliminary analysis of majorization variants according to the «2 of 4» scheme. Analysis of expressions (1)-(3) allows us to conclude that:

option A is inferior to options B and C since there are no means for reserving «2 of 4» elements and connecting systems;

options B and C can compete at certain probabilities of no-failure operation; however, the preferred option for reliability in practice is option C;

as for equipment costs, the best option is option A, then option B, and finally option C.

Thus, preliminary analysis shows that option C is the best in terms of reliability and safety (taking into account the need to meet the requirements of the single failure principle).

Consideration of different connections to sensors

Control systems may have their own sensors and share some sensors with other systems. Therefore, it is necessary to consider different ways of connecting sensors to such systems.

We analyze the following layers: D – sensors, K – communication channels and S – systems:

common redundancy (Figure 9);

distinct redundancy (Figure 10);

distinct bridge redundancy (Figure 11).

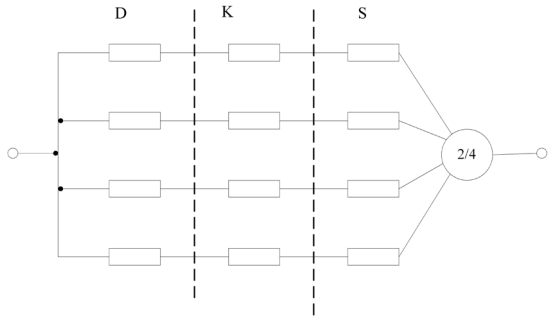

Figure 9 – Common redundancy

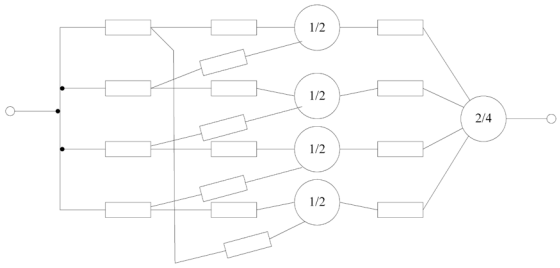

Figure 10 – Distinct redundancy

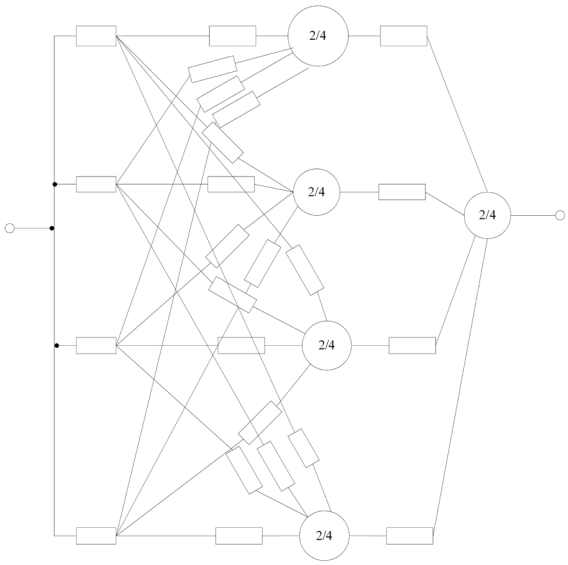

Figure 11 – Distinct bridge redundancy

For structure shown in Figure 9, the expression to find the probability of no-failure operation is the following:

$$P = \sum_{i=0}^{2} C_4^i \left({}_D P_K P_S \right)^{4-i} \left(1 - {}_D P_K P_S\right)^i P_{2/4} \qquad (4)$$

where P_D is the probability of no-failure operation of sensors;

P_K is the probability of no-failure operation of communication channels;

P_S is the probability of no-failure operation of systems;

$P_{2/4}$ is the probability of no-failure operation of voting element;

C_4^i is the number of combinations.

The representation of structures shown in Figure 10 and Figure 11 in formal notations would lead to rather cumbersome expressions. Therefore, engineering calculation software would be appropriate for their analysis. This would be done by the authors in future work.

Acknowledgment

This research is supported by the STARC project (Methodology of SusTAinable Development and InfoRmation Technologies of Green Computing and Communication) funded by the Ministry of Education and Science of Ukraine.

Conclusions

This work shows elements of the reliability and safety assessment technique that considers different ways for the implementation of communications.

The problem relating to the reliability of safety-critical (nuclear power plants and other installations) instrumentation and control systems considering communications includes three subtasks:

first, analysis of communications that significantly influence the reliability;

second, parametrization of communication reliability indicators;

third, correction of reliability diagram to calculate the system reliability.

Future research can be undertaken in the following areas:

further development of the proposed technique taking into account communications within each subsystem;

development of case-based techniques for safety and cybersecurity co-design and assessment [10-13];

specification of instrumentation and control systems considering green IT engineering issues [14].

References

1. Alanen, J., Hietikko, M., Malm, T. (2004). Safety of digital communications in machines. VTT.

2. White, A.J. (2006). An examination of the use of digital communications in safety-related applications. Symp. Series No. 151, pp. 1-17.

3. IEC 61508. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. 2nd ed., IEC.

4. Lee, S.H., Kim, H.E., Son, K.S., Shin, S.M., Lee, S.J., Kang, H.G. (2015). Reliability modeling of safety-critical network

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

communication in a digitalized nuclear power plant. *Reliability Engineering and System Safety*, Vol. 144 (2015), pp. 285–295.

5. Lee, S.H., Kang, H.G., Jung, W.D., Son, K.S. (2017). Risk assessment of safety-critical data communication in digital safety feature control system. NPIC HMIT 2017, pp. 786-795.

6. Yastrebenetsky, M., Kharchenko, V. (2014). Nuclear power plant instrumentation and control systems for safety and security. IGI Global, USA.

7. Reactor power control and limitation system. Retrieved from http://www.radiy.com/en/nuclear/products/fpga-based-safety-and-safety-related-i-c-systems/reactor-power-control-limitation-system-rpcls.html.

8. Rods control system. Retrieved from http://www.radiy.com/en/nuclear/products/fpga-based-safety-and-safety-related-i-c-systems/rods-control-system-rcs.html

9. Myerscough, P.B. (2013). Nuclear power generation: incorporating modern power system practice. Elsevier.

10. Potii, O., Illiashenko, O., Komin, D. (2015). Advanced security assurance case based on ISO/IEC 15408. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Theory and engineering of complex systems and dependability. DepCoS-RELCOMEX 2015. *Advances in Intelligent Systems and Computing*, Vol. 365, pp. 391-401. Springer, Cham.

11. Strielkina, A., Illiashenko, O., Zhydenko, M., Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, pp. 67-73.

12. Kharchenko, V., Illiashenko, O. (2016). Diversity for security: case assessment for FPGA-based safety-critical systems. MATEC Web Conf., 76 p.

13. Illiashenko, O., Kharchenko, V., Brezhniev, E., Boyarchuk, A., Golovanevskiy, V. (2014). Security informed safety assessment of industrial FPGA-based systems. Proceedings of Probabilistic Safety Assessment and Management Conference PSAM 12, 24-27 June 2014, Honolulu, Hawaii, USA, 11 p.

14. Kharchenko, V., Illiashenko, O. (2017). Concepts of green IT engineering: taxonomy, principles and implementation. In: Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (eds) Green IT engineering: concepts, models, complex systems architectures. Studies in Systems, Decision and Control, Vol. 74, pp. 3-19, Springer, Cham.

Аналіз безпеки та надійності ІКС АЕС з урахування різних архітектур комунікацій

Бабешко Є. В.[1,2], Ілляшенко О. О.[1], Харченко В. С.[1, 2], Ручков Є. В. [2]

[1] Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», м. Харків, Україна

[2] Науково-виробниче підприємство «Радій», м. Кропивницький, Україна

Оцінювання безпеки та надійності інформаційно-керуючих систем (ІКС), що застосовуються в різних критичних до безпеки галузях, є відповідальним і складним завданням. Різні моделі оцінювання, рекомендовані міжнародними та національними нормативними документами та використовувані експертами у всьому світі, все ще мають недоліки та обмеження. Отже, є потреба у дослідженнях з вдосконалення та покращення моделей оцінювання. У цій роботі пропонується вдосконалити моделі оцінювання завдяки врахуванню різних архітектур комунікацій як між різними системами, так і в межах однієї системи. В більшості існуючих моделей лінії комунікацій вважаються абсолютно надійними, проте проведений аналіз показує, що їх обов'язково необхідно враховувати. Описано кілька моделей оцінки надійності критично важливих систем для атомних електростанцій з різними комунікаціями.

Ключові слова: ІКС АЕС, імовірність безвідмовної роботи, оцінювання безпеки, оцінювання надійності, комунікації.

Отримано 17.03.2020.