Centrum Rzeczoznawstwa Budowlanego

Open Access Journal
Modern Engineering 1 (2020) 18-25
journal homepage: http://mengineering.eu

MODERN ENGINEERING

Probabilistic Safety Assessment of ESBWR gravity driven cooling system

Aleksej KASZKO[1], Grzegorz NIEWIŃSKI*[1], and Michał STĘPIEŃ[1]

[1]Institute of Heat Engineering, Warsaw University of Technology, Poland

Abstract

According to Polish nuclear law, newly emerging nuclear facilities require probabilistic safety assessment (PSA). This article is intended to present the PSA method and to present the error tree method by which the probability of unavailability of the gravity reactor cooling system (GDCS) of the ESBWR power plant designed by GE Hitachi was determined. This work includes creatiion process of a damage tree and performing a quantitative analysis in SAPHIRE tool and estimating uncertainty using the Monte Carlo method. As a part of the work, it was shown that in the probability of failure of a single GDCS $P_{\text{LINE-A}}$ line, the most important element are the basic events related in particular to the operation of service valves.

Keywords: nuclear power plant, Probabilistic Safety Assessment, PSA, Fault Tree Analysis, FTA, Gravity Driven Cooling System, GDCS.

1 Introduction

Probabilistic Safety Assessment (PSA) is a method used to assess the risk of a specific event occurring [1, 10]. Application for safety assessment in installations with complex technological systems, increased risk, including nuclear power plants [3]. At the nuclear facility, the probabilistic safety assessment method consists of three levels shown in Figure 1 [14, 16]. The PSA method has also extensions in various types, such as Shutdown Probabilistic Safety assessment (S-PSA) [23], Dynamic Probabilistic Safety Assessment D-PSA [11] or Condition-Based Probabilistic Safety Assessment (CB-PSA) [9], but in this article the authors will focus on the basic PSA set.

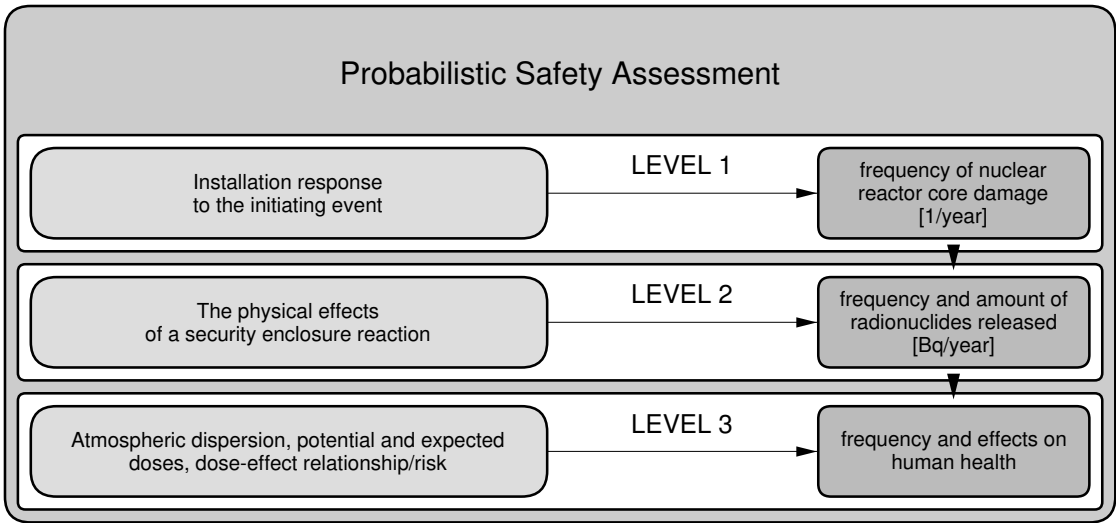

Figure 1. PSA levels

*Corresponding author: E-mail address: grzegorz.niewinski@pw.edu.pl (Grzegorz NIEWIŃSKI)

Received 2 January 2020
Available online 15 March 2020
ISSN 2450-5501
Published by Centrum Rzeczoznawstwa Budowlanego

Level 1

It is used to assess the reliability of security systems based on which the probability of core melting can be estimated. This level provides information on project weaknesses and ways to prevent spinal damage, which in most cases is a precursor to accidents that lead to serious radioactive isotope releases with potential consequences for the environment and human health.

Level 2

It is used to determine the response of the safety enclosure during damage to the core and the frequency of releases. The behavior of the safety enclosure for the heating, production, combustion and explosion of hydrogen as well as the interaction of corium with concrete is examined. Analysis at this level provides additional knowledge about the relative importance of the sequence of failures leading to spinal damage in terms of the severity of radioactive releases. In addition, it provides insight into the weaknesses (and ways to improve) of mitigation and accident management of spinal damage.

Level 3

At this level, the consequences of releasing radioactive material into the environment are analyzed. In addition, public health and social risks such as land, water or food contamination are being assessed. The third level analysis provides knowledge on the importance of accident prevention and mitigation measures expressed in terms of adverse effects on public health and environmental pollution. It also provides information on the relative effectiveness of accident management aspects, creating evacuation plans and methods for undertaking rescue operations.

2 Probabilistic Safety Assessment history

The first applications of Probabilistic Safety Assessment in the field of large-scale nuclear plant safety took place in the 1970s, including such country as United States, Great Britain and Germany.

In 1975, there was created raport WASH-1400 "NUREG 75/014" [20] it was also known as the Rasmussen Report. This document was prepared for the U.S. NRC (United States Nuclear Regulatory Commission) led by Professor Norman Rasmussen and included an assessment of the likelihood of a series of accident sequences that could lead to fuel melting in the reactor (core melting failure) by introducing the error tree method.

In 1978, the NUREG/CR 0400 report [21] was prepared under the direction of Harold Lewis, whose main purpose was to examine the state of the risk assessment methodology and to make recommendations for NRC on how it can be used in the regulatory and licensing process. Areas of research included: risk assessment methodology, statistical issues, completeness, database, and threat assessment carried out in WASH-1400 for human health by radiation arising from a hypothetical accident. Particular attention was paid to issues including: common cause failure; human factor - errors on the service side; earthquake; risk perception, which should be understood as subjective opinions in the risk assessment; the role of probabilistic methods in the regulatory process; calculation of doses for society from released radionuclides.

Research has shown that human errors can have a significant impact on the likelihood of a reactor failure. In addition, the analysis showed the important role of small break Loss Of Coolant Accident (SBLOCA) for pressurized water reactor (PWR), which was confirmed in 1979 by the Three Mile nuclear power plant failure Island. The WASH 1400 report contains information on the strengths and weaknesses of the project, operating procedures for the installations tested, and presents possible ways to improve their safety. PSA research was then carried out at many existing and newly designed nuclear facilities.

Currently, Probabilistic Safety Assessment is used in the licensing process of nuclear installations around the world and has found wide application in other areas of the economy, including in the chemical industry, in the financial, insurance sector, in computer networks, and in other critical infrastructures.

3 Nuclear facility licensing and PSA analysis

According to Polish law - The Act of 29 November 2000 - Atomic Law " [22], an investor who is applying for permission to build a nuclear power plant should submit a Safety Report based on a nuclear facility safety analysis taking into account environmental and technical factors. The prepared document must be verified by an entity that was not involved in the preparation of the report.

The above entry in the Atomic Law shows that in order to obtain a building permit for an object, the operator should carry out, among others full PSA analysis taking into account all possible external factors.

3.1 GDCS system of the ESBWR reactor

Boiling Water Reactor type ESBWR (Economic Simplified Boiling Water Reactor) is a 1520 MWe III + generation reactor. Based on the proven boiling reactor technology (BWR and ABWR), the ESBWR reactor achieved greater design simplicity. Using natural circulation, ESBWR has 25% fewer pumps and mechanical drives than other existing installations. The decrease in the number of auxiliary devices of this type increased the reliability of the installation. According to data provided by GE Hitachi, the probability of damage to the core for this type of reactor is only $1.7 \cdot 10^{-8}[1/year]$ (while the international standard requirement is $10^{-5}[1/year]$). The ESBWR reactor is designed in such a way that it is possible to cool the core in the event of a breakdown, for a minimum of seven days without the operator and external power supply [5, 6, 8, 12].

In the case of a Loss-of-coolant accident (LOCA) failure, which will result in poor heat reception and, as a consequence, may cause the core to melt, the role of the Gravity Driven Cooling System (GDCS) is to provide core cooling in the event of such a failure by supplying additional coolant from the system pools located within the safety enclosure. The system can be seen as two separate subsystems: short-term and long-term security system. Short-term Cooling (Injection) is designed to provide a short-term replenishment of water in the reactor tank to maintain its level above the top of the fuel. In contrast, Long-term Cooling (Equalizing) maintains a constant level of coolant in the reactor tank. Figure 2 shows the GDCS system on the background of the safety enclosure, consisting of the following elements [2]:

- water pools (GDCS Pools, Suppression Pools),
- power lines (GDCS Injection Lines, Equalizing Lines, Deluge Lines),
- explosive and control valves.

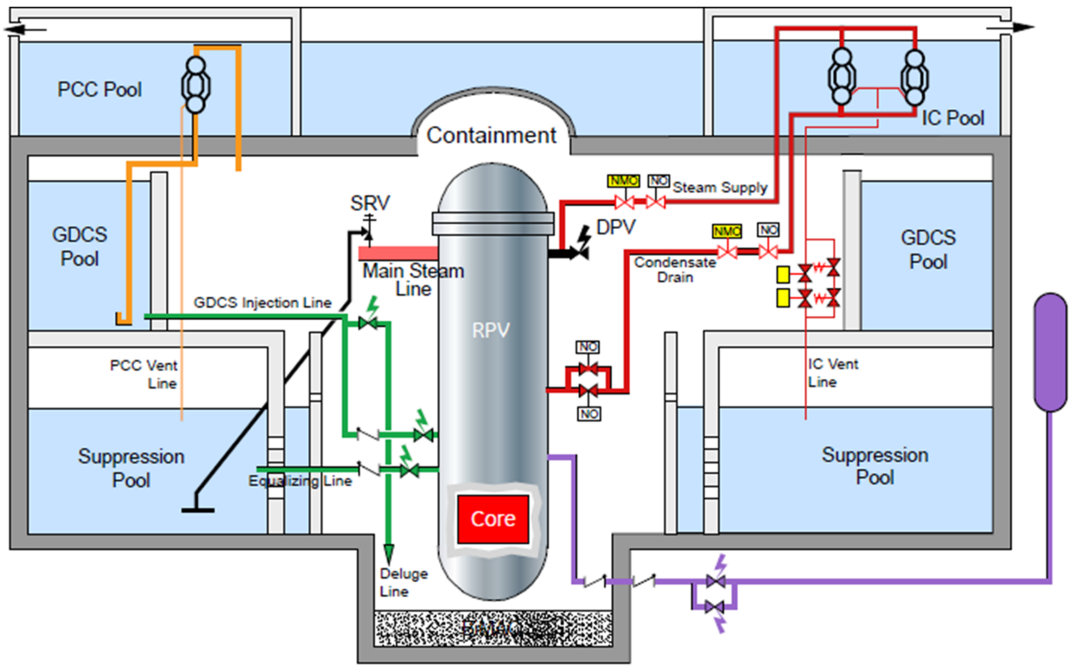

Figure 2. The gravitational cooling system of the ESBWR reactor [7]

The GDCS system uses explosion-proof valves (Squib Valve) characterized by high reliability and short startup time. During the normal operation of the reactor, they remain closed (Figure 3) and are only opened in the event of a failure [4, 7, 13]. The valves are opened by the explosion of pyrotechnic material as a result of an electrical signal from the DCIS (Distributed Control and Information System) control system. After activating the explosive valve, its restoration is required to restore its full functionality.

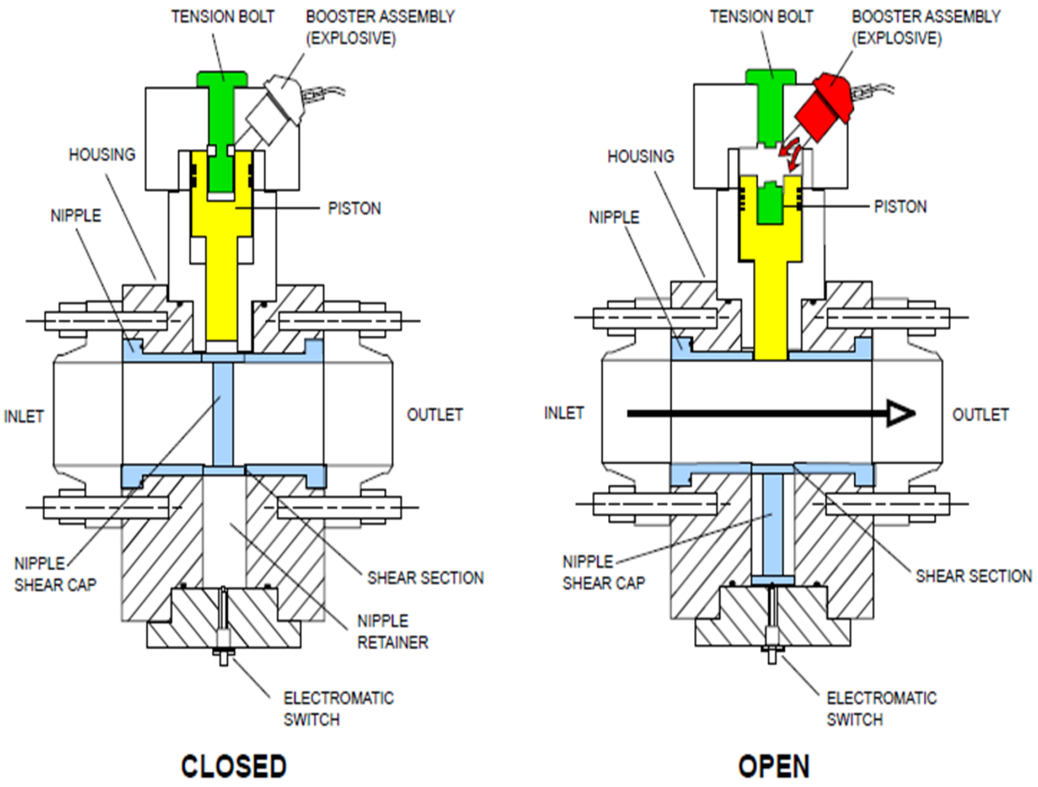

Figure 3. Explosive valve

4 Model of DGCS system in SAPHIRE

SAPHIRE program was developed by Idacho National Laboratory for U.S. and it was used to prepare the error tree of the short-term security system of the GDCS system of the ESBWR reactor. NRC [8, 13, 17–19]. The full system error tree contains 406 basic events and 122 logic gates. Therefore, in this work, in Figures 4-7, selected fragments of the error tree are presented.

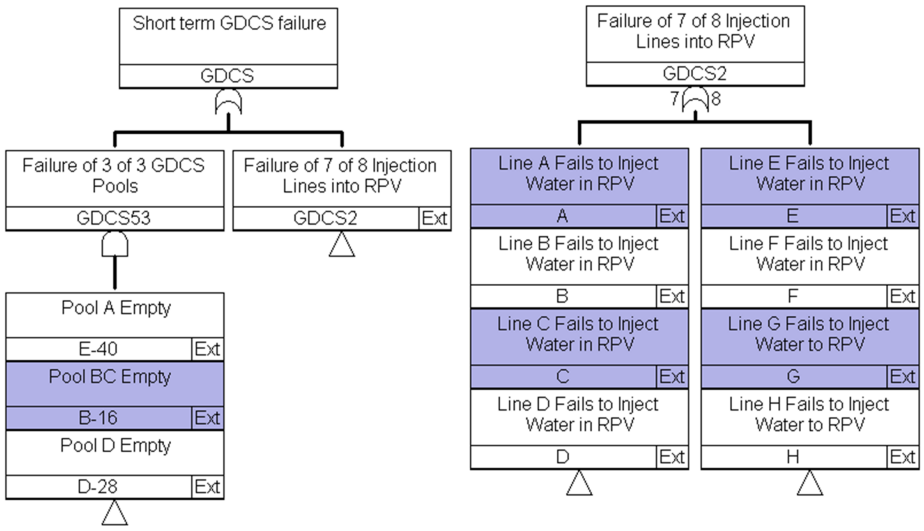

Figure 4. GDCS error tree

The error tree shown in Figure 4 explains how the GDCS system may crash. It can be caused by the simultaneous

failure of all three pools (A, BC, D) or by the failure of seven out of eight lines (lines A-H) injection into the reactor tank (RPV).

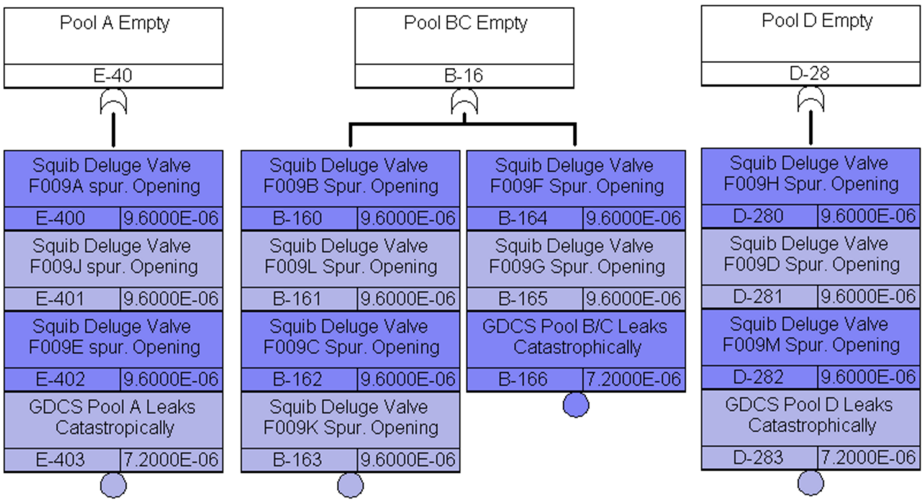

Figure 5. GDCS error tree (continuation)

Figure 5 shows the error trees for pools A, BC and D (the pool is empty). They show that a fault, e.g. pool A, can occur through a significant leakage of water from a leaking pool (event E-403) or by unwanted opening of one of the explosive valves (events E-400 - E-402).

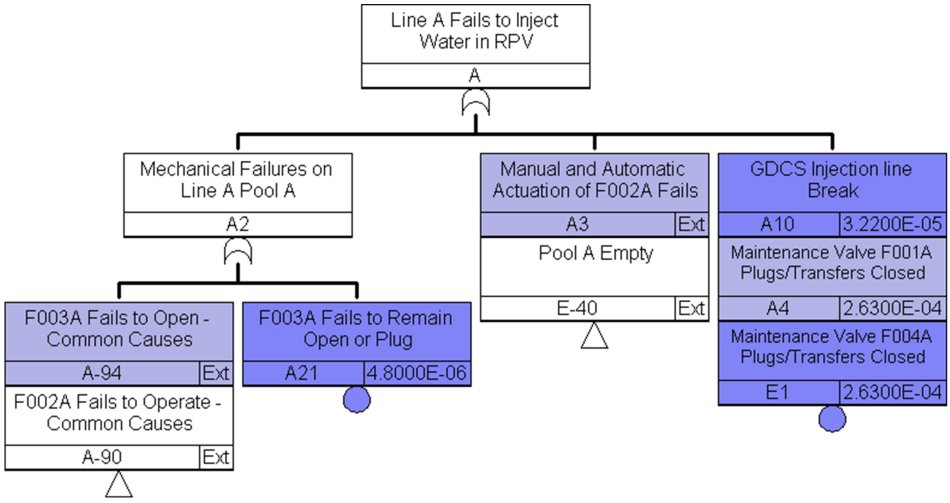

Figure 6. GDCS system for A line failure

Figure 6 shows an example of an error tree for injection line A failure. The reason for incorrect operation of the injection line may be mechanical faults on the line (event group A2), rupture (event A10), failure of manual and automatic actuation of the explosion valve (event A3), leaving valves closed (event A4 and E1) or empty pool (event E-40). Figure 7 shows the expansion of the A3 subtree.

The calculation algorithm of the PSA method using the SAPHIRE program consists of several stages. In the first step, each elementary event from the error tree (e.g. valve failure, line unsealing, etc.) is assigned based on a database provided by the U.S. NRC, baseline failure probability. In the next step, during the simulation, using the Monte Carlo method [15], the fault factor (EF) is randomly drawn, then the final probability of an elementary event is determined based on its value and the base value of failure probability. The final stage of calculations is the logical analysis of the error tree determining the probability of failure of the entire system. Repeated execution of the above algorithm enables the system failure probability distribution to be obtained, as shown in Figures 8-9 [17].

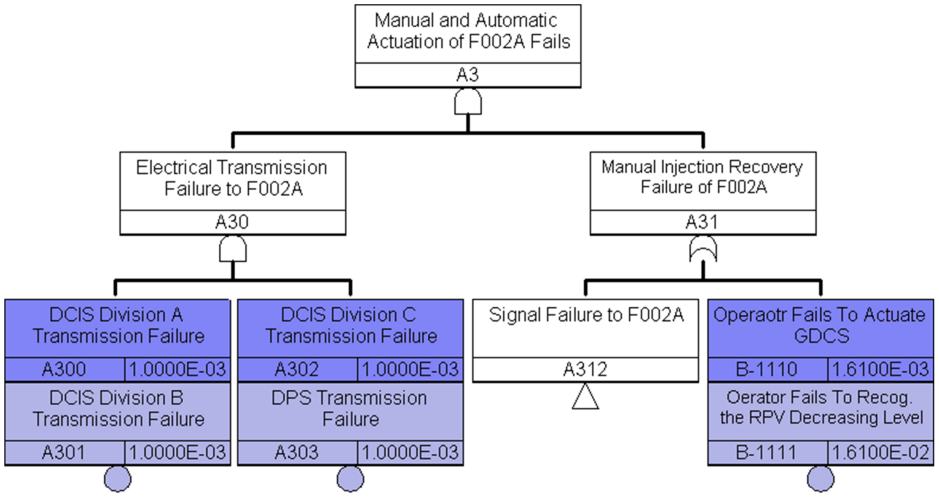

Figure 7. GDCS system A line failure (continued)

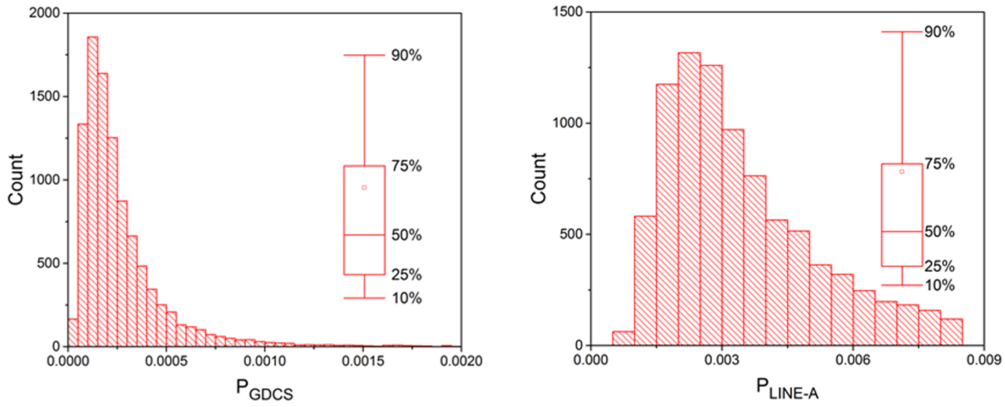

Figure 8. Distribution of failure probability in the injection phase (P_{GDCS}) and failure probability of a single line (P_{LINE-A})

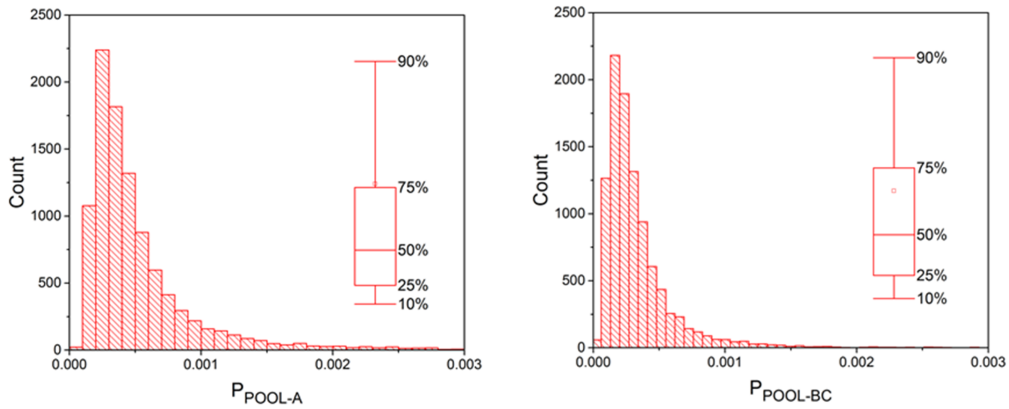

Figure 9. Distribution of failure probability of two redundant lines with a shared pool (P_{POOL-A}), four redundant lines with a shared pool ($P_{POOL-BC}$)

Figures 8 and 9 show the distribution probability of system failures and selected components for 10,000 draws. The abscissa indicates the probability of failure of a given system or subsystem, and the ordinate shows the number of counts for the given probability. Analyzes have shown that the probability of GDCS failure in the injection phase

is $2 \cdot 10^{-4}[1/year]$. The low probability value was achieved by limiting the number of auxiliary devices (e.g. pumps) and multiplying subsystems (i.e. 3 swimming pools, 8 supply lines).

5 Conclusions

PSA is a worldwide method used when licensing nuclear facilities are created. Its main advantage is the ability to determine the probability of failure of the selected system and estimate the probability of damage to the core. In addition, it allows to understand what factors/elements make the greatest contribution to the probability of a failure. In the probability of failure of a single GDCS (P_{LINE-A}) line, the main events related to service valves made the largest contribution.

References

1. *Applications of probabilistic safety assessment (PSA) for nuclear power plants* (International Atomic Energy Agency, Vienna, Austria, 2001).
2. Bilbao, Y. & Leon, S. *Natural Circulation Phenomena for Passive Safety Systems of Advanced Water Cooled Reactors, IAEA/ICTP Workshop on Nuclear Reactor Data for Advanced Reactor Technologies ICTP, Tieste, May 3-14* 2010.
3. Chmieliński, M. Inspection of Containers of the Explosives Materials in the Maritime Transport. *Inżynieria Bezpieczeństwa Obiektów Antropogenicznych* **3.** ISSN: 2450-1859 (2019).
4. Fries, D. & Tietsch, W. *AP1000 Nuclear Power Plant – Passive Safety System Actuation using Explosively Opening "Squib Valve"* in *booktitle* International Conference on Opportunities and Challenges for Water Cooled Reactors in the 21st Century (Vienna, 2009).
5. *GE Hitachi, ESBWR Passive Safety Fact Sheet* (2011).
6. *GE Hitachi, The ESBWR Plant General Description* (2011).
7. *GE Nuclear Energy, ESBWR Design Description, NEDC-33084 – Document Transmittal for Pre-Application Review of ESBWR* 2002.
8. Hinds, D. & Maslak, C. *Next-generation nuclear energy:The ESBWR* (2006).
9. Hoseyni, S. M., Maio], F. D. & Zio, E. Condition-based probabilistic safety assessment for maintenance decision making regarding a nuclear power plant steam generator undergoing multiple degradation mechanisms. *Reliability Engineering and System Safety* **191,** 106583. ISSN: 0951-8320 (2019).
10. Kaszko, A., Niewiński, G. & Stępień, M. Reliability Analysis Of ESBWR Gravity Driven Cooling System. *Aparatura Badawcza i Dydaktyczna* **3,** 191–198 (2017).
11. Lee, H., Kim, T. & Heo, G. Application of Dynamic Probabilistic Safety Assessment Approach for Accident Sequence Precursor Analysis: Case Study for Steam Generator Tube Rupture. *Nuclear Engineering and Technology* **49,** 306 –312. ISSN: 1738-5733 (2017).
12. Lim, J. *et al.* Assessment of passive safety system performance under gravity driven cooling system drain line break accident. *Progress in Nuclear Energy* **74,** 136 –142. ISSN: 0149-1970 (2014).
13. *Multinational Design Evaluation Programme, The design and use of explosive-actuated (squib) valves in nuclear power plants* 2010.
14. Nasbaumer, O. *Introduction to Probabilistic Safety Assessments (PSA)* ().
15. Oh, K. *et al.* Study on Quantification Method Based on Monte Carlo Sampling for Multiunit Probabilistic Safety Assessment Models. *Nuclear Engineering and Technology* **49,** 710 –720. ISSN: 1738-5733 (2017).
16. *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms: A Safety Practice Safety Series* **50-P-8.** ISBN: 92-0-102195-X (International Atomic Energy Agency, Vienna, 1995).
17. Smith, C., Wood, S. & O'Neal, D. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8: User's Guide* (Idaho National Laboratory, 2011).
18. *U.S. NRC, Inductry Averange Parameters Estimates, Component Reliability* 2015.
19. *U.S. NRC, Industry-Averange Performance for Components And Initiating Events at U.S. Commercial Nuclear Power Plants (NUREG/CR-6928* 2007.
20. *U.S. Nuclear Regulatory Commission, Reactor Safety Study, An assessment of accident risks in U.S. Commercial Power Plants* 75/014 (NUREG).
21. *U.S. Nuclear Regulatory Commission, Risk Assessment Review Group Report* NUREG/CR-0400.
22. *Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe, Dz.U.2017.0.576*

23. Čepin, M. Application of shutdown probabilistic safety assessment. *Reliability Engineering and System Safety* **178,** 147 –155. ISSN: 0951-8320 (2018).