Co-simulation for real time safety verification of nuclear power plants

Emmanuel BOAFO*, Elnara NASIMI*, Luping ZHANG* and Hossam A.GABBAR**

*Faculty of Engineering and Applied Science, University of Ontario Institute of Technology
2000 Simcoe Street North, Oshawa, Ontario L1H 7K4, Canada

**Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology
2000 Simcoe Street North, Oshawa, Ontario L1H 7K4, Canada

E-mail: Hossam.gabbar@uoit.ca

Received: 29 September 2015; Revised: 28 December 2015; Accepted: 20 March 2017

Abstract
Small and major accidents and near misses are still occurring in nuclear power plants (NPPs). Risk level has increased with the degradation of NPP equipment and instrumentation. In order to achieve NPP safety, it is important to continuously evaluate risk for all potential hazard and fault propagation scenarios and map protection layers to fault / failure / hazard propagation scenarios to be able to evaluate and verify safety level during NPP operation. There are major limitations in current real time safety verification tools, as it is mainly offline and with no integration to NPP simulation tools. The main goal of this research is to develop real time safety verification with co-simulation tool to be integrated with plant operation support systems. This includes the development of static and dynamic fault semantic network (FSN) to model possible fault propagation scenarios and the interrelationships among associated process variables. The detailed methodology involves the integration of process models, construction of static FSN with fault propagation scenarios, and evaluation and tuning of dynamic FSN with probabilistic and process variable interaction values. The focus however of the present study is to highlight the need to incorporate error reduction in performing safety verification of NPPs. Two selected case studies were used to demonstrate the proposed methodology; one on a turbine trip and the other on steam generator tube rupture. In the former case, the error reduction concept was shown while the safety verification method was demonstrated in the latter case. The results confirmed the importance of error reduction as well as the need to constantly undertake safety verification of safety critical systems such as a NPP.

Key words: Fault Semantic Network, Safety verification, NPP, Fault propagation, Risk

1. Introduction

The safety of Nuclear Power Plants (NPPs) is a major concern to all due to its importance. Assuring the safety of a NPP is a key objective of all stakeholders. Considering previous accidents in NPPs such as Chernobyl, TMI and recently in Fukushima, the need to review existing safety system designs and their operation is justified as a means of verifying the performance of these systems in order to prevent future accidents. In NPPs, safety systems are represented in the form of independent layers of protection or barriers. These layers are expected to prevent or reduce the effects of all possible hazard scenarios. Typical safety systems are represented within process control systems such as alarms, process limits or control rules, which are translated into control actions (Gabbar, 2010). An effective safety control design can improve plant operation economics, by optimizing safety margins to reduce unnecessary shutdown cases (O’Hara, 1994). This also takes into account human factors involved in plant operation in order to ensure that safety margins are matched with required operator actions (Moray and Huey, 1988; Lee and Seong, 2004).

Faults are abnormal conditions where deterioration occurs to plant equipment/process that can be caused by various factors including human errors, environmental stresses or material deficiencies (Gabbar, 2007). Fault diagnosis and safety verification are important for the operation of nuclear power plants in terms of their safety and cost effective operation. Mostly, fault diagnostic approaches are based on the sensors that measure important process variables. Faults usually propagate and may result in accidents if not diagnosed and appropriate action taken in a timely manner. Safety verification...
is therefore linked with accurate fault diagnosis and propagation analysis.

In the TMI accident, a relief valve failed to close after it opened automatically in response to a failure of water pumps. This failure led to loss of coolant from the reactor core and the fuel rods inside the reactor experienced a partial meltdown. Operators at the plant didn’t receive the signal that the valve had not closed. This accident was as a result of a combination of equipment malfunctions, design-related problems and human errors (US-NRC, 1979). In the above situation, the accident could have been prevented if the safety instrumented system responsible for the detection and display of the relieve valve malfunction had been verified.

During a test of reactor response to electrical failure in the Chernobyl plant by operators, a design flaw in the reactor caused a power surge that resulted in an uncontrolled nuclear chain reaction. This led to two explosions that sent a radioactive plume to the atmosphere as a result of the absence of a containment building. The accident could have been prevented if the reactivity temperature coefficient had been negative during reactor design. Furthermore, adhering to a proper safety procedure would have ensured that the reactor was shut down before carrying out such a test.

Emergency cooling systems failure at the Fukushima Daiichi plant after a massive earthquake and tsunami led to a station blackout. The lack of cooling of the fuel rods led to their meltdown in multiple reactors. This accident resulted in some fatalities and contaminated large areas (Zhu et al., 2014). Explosions occurred in some of the plant units as a result of the buildup of hydrogen gas. A probability risk assessment conducted on the plant site would have identified the eminent potential of a tsunami occurring at the site and this hazard would have been mitigated as part of a risk reduction strategy.

The above accidents attest to the fact that safety verification of NPPs need to be continuously conducted and results updated with changing plant conditions. Verification is the evaluation of an implementation to determine that applicable safety-critical requirements for any plant and its operations are met. The verification process ensures that the design solution meets all validated safety requirements (Rastogi and Gabbar, 2012). A verified system shows measurable evidence that it complies with the overall system safety needs by incorporating an integrated framework.

It has been identified that there exist discrepancies between the results of codes that have been designed to simulate faults and transients in NPPs such as CATHENA/RELAP5 (Hanna et al., 1995) on the one hand and then real time data available from the plants’ operation. An example of steam generator level in Canadian Deuterium Uranium (CANDU) reactor is shown in table 1 to demonstrate that the difference between two states is within the error between real time and simulation results.

<table>
<thead>
<tr>
<th>Table 1. SG levels of CANDU.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Full Power</td>
</tr>
<tr>
<td>Level High Alarm</td>
</tr>
<tr>
<td>CATHENA</td>
</tr>
<tr>
<td>Real Time</td>
</tr>
</tbody>
</table>

*CATHENA & Real Time (Choi et al., 2001), Full Power & Level Alarm (Nasimi and Gaber, 2011)*

These differences may lead to differences in time taken to reach limits and that poses a problem for a suitable response action. Subsequently, this affects the accuracy of fault propagation prediction and the relationship between process variables is also affected. Fault propagation is affected in terms of speed and the strength between process variables.

Currently, faults are detected in a nuclear power plant such as CANDU by the use of alarm and annunciation windows on the plant control console and the reading of parameter changes from the console by operators. However, these do not give adequate information on causes and consequences of faults. In a previous work (Gabbar and Boafo, 2014), some of the above issues were mentioned and an error reduction method was presented and discussed. The current paper extends the earlier work with a focus on the safety verification aspect and the addition of the steam generator steam rupture scenario.

2. Literature review

Several methods have been extensively utilized and reported for fault diagnosis and safety verification of complex systems
such as nuclear power plants, aircrafts, chemical processing plants and space vehicles. These methods include the following; fault tree analysis (FTA) (Haasl, 1965). FTA can be used to detect causes of faults and their subsequent propagation, however FTA is limited because it is implemented manually and not suitable for real-time fault diagnosis (Nasimi and Gabbar, 2014). Zhao and Upadhyaya (2006) and Gross et al. (1997) also used model based methods for fault diagnosis. The sign directed graph (SDG) is a logic based method (Iri, 1979) that can be used to perform fault diagnosis. Although SDG is a useful method for fault diagnosis and propagation, its usage is unattractive since it requires robust mechanisms to construct fault models (Gabbar, 2007). Data-driven solutions based on computational intelligent methodology have gained popularity in fault diagnosis of nuclear power plants. They include, Artificial Neural Networks (ANN), Genetic Algorithms (GA), fuzzy logic and Neuro fuzzy techniques. These computationally intelligent methods have been widely used in recent times due to their learning abilities for fault diagnosis and their inherent parallel structures. They have therefore been applied in different types of industries including geophysical (Sandham and Legget, 2003), oil and gas (Gabbar, 2010) and in nuclear steam supply system of a nuclear power plant (Hadad et al., 2008; Xin et al., 2010). The structured identification of faults, causes and consequences is a major problem in fault diagnosis (Gabbar, 2007)

2.1. Fault detection and diagnosis
This refers to the condition that every fault defined for the process has to be observed by at least one sensor. For a given process, the observability problem becomes finding the minimum number of sensors that would cover all faults (root nodes). This is commonly known as minimum set covering problem (Upadhyaya et al, 2011). Resolution refers to the ability to the ability to identify the exact fault that has occurred. The fault observability and resolution could be solved by linking the root nodes and sensor locations, but this becomes difficult due to increasing number of faults and sensor locations. Heuristics often give a quick and reasonably accurate solution. A greedy search heuristic was developed for solving the single and multiple fault observability and resolution problem as reported in (Raghuraj et al., 1999, Bushan et al., 2000). Not all faults are distinguishable by using the sensor placement sets obtained from the above method. However, these methods provide essential information to the PCA-based FDI system.

2.2. Protection layers and defence-in-depth
In NPPs, safety is achieved by the implementation of various barriers that are meant to ensure that processes are carried out in a safe and reliable manner and also to prevent and control any abnormal/accident conditions that may occur as well as to mitigate any consequences of accidents if they occur. This is the defence-in-depth concept. Safety protection layers are mapped to defence-in-depth levels in which each defence-in-depth level should be covered by more than one protection layer. Independent protection layers (IPLs) include: IPL1: safety design; IPL2: basic process control/alarm; IPL3: critical alarm; IPL4: safety instrumented system (SIS); IPL5: relief devices; IPL6: physical protection; IPL7: site emergency procedures; and IPL8: community protection (Gabbar, 2010).

3. PROPOSED METHODOLOGY
3.1. Fault Semantic Network
Fault Semantic Network (FSN), developed by (Gabbar, 2007), is used to represent fault knowledge based on connections between objects. FSN is used in this study to construct fault propagation scenarios in order to enhance the performance of the Fault diagnostic systems and to achieve real time safety verification of NPPs. FSN is constructed based on ontology structure of fault models based on process object oriented methodology (POOM) in which failure mode (FM) is described using symptoms, enablers, variables, causes and consequences. Rules are associated with each transition of the causation model in FSN. For example, failures related to loss of feedwater might be associated with rules such as the one explained below.

FSN Rule Structure.

IF (Structure= steam Generators) And (PV= SG Level) And (Dev= Low feedwater flow)
THEN (FM= Loss of feedwater)

Where PV is process variable and Dev is deviation.

Formal language is proposed to represent process domain knowledge and safety control rules as explained in Gabbar (2007). These rules are initially defined in generic form based on domain knowledge, i.e. regardless of plant specific knowledge and then further explained for plant specific knowledge based on observations. A risk element is identified for each hazard or fault propagation scenario from the root causes to the final consequences. Three possible risk elements associated with consequence-1 can be represented as follows,

- Cause-1 → failure-1 → consequence-1
- Cause-2→ failure-1→ consequence-1
- Cause-3 → failure-1→consequence-1

For independent events, the total risk associated with consequences 1, 2 and 3 are represented in Eqns. 1, 2 and 3.

\[
\text{Risk (Consequence-1)} = [(\text{CaFr}_1+\text{CaFr}_2+\text{CaFr}_3) \times \text{FPr}_1 \times \text{CoPr}_1] \times \text{Colm}_1 \\
\text{Risk (Consequence-2)} = [(\text{CaFr}_1+\text{CaFr}_2+\text{CaFr}_3) \times \text{FPr}_2 \times \text{CoPr}_2] \times \text{Colm}_2 \\
\text{Risk (Consequence-3)} = [(\text{CaFr}_1+\text{CaFr}_2+\text{CaFr}_3) \times \text{FPr}_3 \times \text{CoPr}_3] \times \text{Colm}_3
\]

Where,
- \(\text{CaFr}_1\) = frequency of cause-1
- \(\text{FPr}_1\) = Probability of failure-1 occurring as a result of any cause.
- \(\text{CoPr}_1\) = Probability of consequence-1 occurring.
- \(\text{Colm}_1\) = Total impact of consequence-1.

For dependent events, Bayesian theorem can be used to determine the total risk based on dependencies for cause-1, 2 and 3.

The proposed FSN consists of two parts of static off-line and dynamic online models. Static FSN comprises faults, failures, hazards and accidents that are linked in the form of causation models associated with process equipment while dynamic FSN involves the use of dynamic simulated or real time data that can be obtained from sources such as, operation, maintenance, safety and control. In this study, static FSN is constructed for different fault propagation scenarios after which operational scenarios for different fault propagation scenarios from real time data or simulation are identified. The FSN methodology will help in addressing current issues in the Nuclear Power Industry such as, low accuracy of fault diagnosis, lack of understanding of process variable interaction by plant operators and human errors that may arise as a result of a combination of these factors. Fig. 1 shows the FSN model for a NPP representing a turbine trip in which \(\Delta T\) stands for the time taken between the occurrences of two events while Fig. 2 shows the activity model of Process Safety Management, which includes safety verification.

The proposed FSN when implemented as an operational support tool is expected to give more information to an NPP operator regarding fault propagation as well as risk estimation for a particular plant state.
3.2. Safety verification

Safety verification forms part of procedures used in performing safety life cycle activities of a process. The various steps are shown in Fig. 2 and briefly described below.

- Hazard and Operability Study (HAZOP)
- Failure Mode and Effect Analysis (FMEA)
- Fault Semantic Network (FSN)
- Predict mechanical, electrical, thermal hazards
- IAEA Standards
- CNSC regulations
- LOPA
- Passive Safety design
- Inherent safety design
- Emergency preparedness

Fig. 1. FSN model for NPP

Fig. 2. Activity model of Process Safety Management based on IEC61508
3.3. **Hazard identification**

This step entails identification of possible hazards associated with the operation of a NPP. Both qualitative and quantitative methods are used such as HAZOP, FTA and FMEA. It includes electrical, thermal, neutronic, radiological or environmental hazards that can occur as a result of operating the NPP.

3.3.1. **Risk assessment/evaluation**

Risk estimation methods can be classified as quantitative, qualitative or hybrid. Risk associated with a particular event can be defined as the product of the probability of the event occurring and the magnitude of consequences resulting from the event.

\[
Risk = Hazard \text{ frequency} \times Hazard \text{ consequence}
\]

Risk assessment consists of qualitative identification, characterization and ranking hazards and qualitative risk evaluation; calculating likelihood frequencies and consequences of hazards. Proportional Risk Assessment Technique (PRAT), Probability Safety Assessment (PSA) are some methods used to perform risk assessment.

3.3.2. **Safety requirements specification**

This usually involves the link between Independent Protection Layers (IPLs) and the concept of defence-in-depth applicable to NPP operation in this case. Safety requirements are outlined by various standards and codes including, IEC61511 and IEC61508 for energy and production plants, IAEA standards and guides are also used for safety requirement specification in the nuclear industry. In nuclear power plants, the link between safety requirements and protection layers involves a mapping of defence-in-depth levels unto IPLs as illustrated in Fig. 3, where the IPLs are described as follows, IPL1: process design, IPL2: basic controls, process alarms and operator supervision, IPL4: Automatic SIS, IPL5: physical protection (relief devices), IPL6: physical devices (containment dikes) and IPL7: plant emergency response.
3.3.3. **Inherent safety design**

This is achieved by changing process design for safety purposes. For instance, in the nuclear power plant, the reactivity temperature coefficient is designed to have a negative value. This characteristic of the plant ensures that the reactivity and for that matter the power of the reactor decreases in the event of temperature increase in order to avoid likely accidents.

3.3.4. **Safety verification**

This involves comparing the calculated risk to the target risk in order to determine whether a process is safe or unsafe. Safety verification is carried out in view of the safety requirements set out by the IAEA and other regulatory bodies. A calculated risk below the target risk implies the process is safe while actual risk higher than the target risk means the process is unsafe and risk reduction methods need to be implemented.

3.3.5. **Risk reduction**

This is needed if the calculated risk is greater than the target risk. It can be achieved by various methods including, passive safety, inherent safety, operator training and emergency preparedness. Risk reduction generally involves the deployment of several barriers between initiating events and final consequences.

4. **Case study**

4.1. **Fault propagation scenarios**

We consider the fault propagation of a Turbine trip and a Steam Generator Tube Rupture for our analysis. The fault...
propagation scenarios are summarized in Fig. 4 and Fig. 5.

4.1.1. **Turbine trip**

A Turbine trip results in temperature and pressure increase in the SG shell as well as an initial increase in coolant temperature and pressure. The Emergency stop Valves (ESVs) and Governor Valves (GVs) are closed immediately after a Turbine trip. This is to stop steam flow to the Turbine, the Condenser Steam Discharge Valves (CSDVs) and the Atmospheric Steam Discharge Valves (ASDVs) are then open to bypass steam to the condenser and the atmosphere respectively. It is expected that the Steam Discharge Valves (SDVs) work properly to prevent a reactor trip or the opening of MSSVs.

A reactor trip is undesirable because it leads to loss of electrical power to the grid and could be a very huge financial loss. Also a reactor trip may lead to loss of offsite power and both of these situations are extremely undesirable.

![Fig. 4. Fault propagation scenario Turbine trip.](image)

4.1.2. **Steam generator tube rupture**

During the operation of a NPP, several initiating events may lead to the propagation of faults in various components. Steam Generator Tube Rupture (SGTR) is a phenomenon that is essential for consideration in performing safety assessment of SG integrity due to its degradation. PRA has been prescribed by the USNRC (NUREG-1570) for estimating the risks associated with operating a degraded SG. In this study, some results obtained from a PRA of SG integrity were used to perform safety verification of NPP based on some selected fault propagation scenarios.
Fig. 5. Fault propagation scenarios for Steam Generator Tube Rupture.

Safety systems are designed as part of the plant to prevent the occurrence of initiating events. If however these events do occur, there are still safety systems that act as Independent Protection Layers (IPLs) to check the propagation of faults. The vertical lines in Fig. 5 represent some of these IPLs which can be in the form of passive safety systems, inherent safety design or active safety systems. An initiating event may either lead to faults/failures or be curtailed by safety systems.

Fig. 5 depicts some fault propagation scenarios that may result in large releases of fission products following the rupture of SG tubes. These releases may result from core damage if protection layers or systems fail. The first fault propagation scenario involves the occurrence of SGTR followed by loss of reactor cooling system (RCS) and core heat removal. This scenario requires once-through cooling, if it fails, a high RCS pressure early core damage occurs.

The second fault propagation scenario starts with SGTR occurring followed by a successful reactor trip and primary-secondary heat removal. The RCS however remains at high pressure and coolant inventory is assumed to be lost. RCS inventory control will be lost following the depletion of the Reactor Water Safety Tank (RWST). The High Pressure Safety Injection (HPSI) suction will be aligned to an empty containment sump. This scenario leads to a late core damage.

4.2. FSN dynamic update

Fault propagation scenarios are defined based on historical data initially and later updated using real time data. Changes in plant conditions and states can be modeled by the FSN. In the dynamic FSN, new data obtained from sensors or by running simulations is used to update process variables by implementing a reasoning process. The reasoning process enables the mapping between process variables both qualitatively and quantitatively. The reasoning maybe diagnostic, predictive, inter-causal or combined. In diagnostic reasoning, symptoms of a fault are first identified and the likely causes are obtained as output of the reasoning. A low steam generator level maybe considered a symptom and a low feedwater flow or irrational flow sensor maybe likely causes.

In predictive reasoning, faults are predicted without the knowledge of symptoms. For example, decreasing the feedwater control valve will result in low steam generator level. In inter-causal reasoning, multiple causes result in a single consequence. In combined reasoning, a combination of any or all the other types of reasoning is used to achieve the desired outcome.
4.3. Co-simulation with improved models

This involves the use of error models incorporated into multiphysics codes to reduce the difference between simulation and real time to construct the dynamic FSN. In this way, fault propagation analysis is expected to be more accurate as it will be closer to real time. The co-simulation with reduced error will be used to establish the process variable deviation interactions.

5. Results and discussion

5.1. Error reduction

It can be seen from Figs. 6-8, simulation results do not match real time data for the turbine trip case study and as demonstrated in table 1, these differences can be within control or safety limits and may have implications on response actions in the event of reactor transients. In Fig. 9 however, a reduction is noticed in the error between simulation results by CATHENA and real time data after incorporating an error function. This error reduction is expected to go a long way in improving the accuracy of simulations in predicting fault propagation.

The error function used for reducing the error in Fig. 7 is given by Eq. 4.

\[ EF = 0.0004x^3 - 0.0064x^2 + 0.0153x - 0.0544 \]  

(4)

where ‘x’ is the time after the Turbine trip.

The mean absolute error (MAE) is given by Eq. 5,

\[ MAE = \frac{\sum_{i=1}^{n} |y_i - \bar{p}_i|^2}{n} \]  

(5)

Where \( y_i \) and \( \bar{p}_i \) are the real time outputs and the average of the outputs of the models respectively.

![Fig. 6. Comparison of Simulation and CATHENA results following a Turbine trip.](image-url)
5.2. Risk estimation for SGTR

Safety verification involves a comparison between the total risk associated with a process and the target risk. The target risk is usually set by the regulatory body such as the USNRC, CNSC or the IAEA. Risk estimation methods described earlier were used to estimate the total risk associated with the fault propagation scenarios identified. This result was then compared with the risk target set by the USNRC for safety verification. In estimating the risk for a fault propagation scenario, the following equation was used.

\[
Risk(path - i) = R_i \times PFDi \times \ldots \times R_n \times PFDn
\]

(6)

Where the meaning of the terms are described in Table 2.
### Table 2 Risk estimation parameters

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Magnitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Steam Generator Tube Rupture</td>
<td>2.7</td>
</tr>
<tr>
<td>R2</td>
<td>Early core damage</td>
<td>5.5E-08</td>
</tr>
<tr>
<td>R3</td>
<td>Late core damage</td>
<td>5.5E-08</td>
</tr>
<tr>
<td>R4</td>
<td>Loss of RCS/LOCA</td>
<td>2.4E-15</td>
</tr>
<tr>
<td>PFD1</td>
<td>Probability of failure on demand of IPL1</td>
<td>0.05</td>
</tr>
<tr>
<td>PFD2</td>
<td>Probability of failure on demand of IPL2</td>
<td>0.01</td>
</tr>
<tr>
<td>PFD3</td>
<td>Probability of failure on demand of IPL3</td>
<td>0.0045</td>
</tr>
</tbody>
</table>

The total risk estimation is given as,

\[
Total\ Risk = \sum_{i=1}^{n} Risk(path - i) \tag{7}
\]

From Eq. 5, the risk associated with fault propagation path 1 is estimated as,

\[
Risk(path - 1) = R_1 \times PFD1 \times R_2 \times PFD2 \times R_3
\]

\[
= 2.7 \times 0.05 \times 5.5E - 08 \times 0.01 \times 5.5E - 08
\]

\[
\approx 4.08E - 18
\]

Risk associated with fault propagation path 2 is estimated as,

\[
Risk(path - 2) = R_1 \times PFD1 \times R_2 \times PFD2 \times PFD3 \times R_4
\]

\[
= 2.7 \times 0.05 \times 5.5E - 08 \times 0.01 \times 5.5E - 08 \times 0.0045 \times 2.4E - 15
\]

\[
\approx 4.41E - 35
\]

Therefore, the total risk is estimated from Eq. 6 as,
\[ Total \ Risk = Risk(path - 1) + Risk(path - 2) \]
\[ \approx 4.08E - 18 + 4.41E - 35 \]
\[ \approx 4.08E - 18 \]

The USNRC safety goal states that the cancer fatality risk associated with exposure from NPP accidents to the population near an operating NPP should not exceed one-tenth of one percent (USNRC). The target risk considered in this study therefore was 1.0E-03.

The safety verification method demonstrated above is expected to form part of the dynamic FSN model for possible deployment in real time. This can be utilized as an operator support tool that will enhance plant safety by providing insights into risk levels associated with various plant states. In this way, both regulators and operating organizations of NPPs can make use of the approach in verifying plant safety and executing preventive maintenance activities.

6. Conclusion

In this paper, we have discussed the use of FSN methodology that can be implemented for co-simulation in a nuclear power plant to enhance fault detection and propagation analysis. Selected case studies of Turbine trip and Steam Generator tube rupture were considered. The need for incorporating error reduction between simulation models and real time data has been highlighted. The mean absolute error values calculated confirmed the accuracy and precision of the error model used within a certain time interval for a particular process variable.

The safety verification results for the Steam Generator tube rupture indicate that the process was safe under the assumptions and the scenarios considered. This result is however not an assurance of plant safety at all times and under all conditions. The framework presented can be implemented constantly to account for plant states which would change with time. Safety verification performed constantly is expected to identify eminent risks and with appropriate risk reduction methods implementation, the overall safety of any process will be greatly enhanced.

References


