Formal Probabilistic Risk Assessment of a Nuclear Power Plant

Mohamed Abdelghany
m_eldes@ece.concordia.ca
Department of Electrical and Computer Engineering,
Concordia University, Montreal, QC, Canada.

Sofiène Tahar
tahar@ece.concordia.ca
Department of Electrical and Computer Engineering,
Concordia University, Montreal, QC, Canada.

Abstract

Functional Block Diagrams (FBD) are commonly used as a graphical representation for probabilistic risk assessment in a wide range of complex engineering applications. An FBD models the stochastic behavior and cascading dependencies of system components or subsystems. Within FBD-based safety analysis, Event Trees (ET) dependability modeling techniques are typically used to associate all possible risk events to each subsystem. In this paper, we conduct the formal modeling and probabilistic risk assessment of a nuclear power plant in the HOL4 theorem prover. Using an FBD modeling in HOL4 of the nuclear Boiling Water Reactor (BWR), we formally determine all possible classes of accident events that can occur in the BWR. We compare our formal analysis in HOL4 with those obtained analytically and by simulation using Matlab and the specialized Isograph tool. Experimental results showed the superiority of our approach in terms of scalability, expressiveness, accuracy and CPU time.

CCS Concepts: • **Computing methodologies** → **Modeling and simulation**; *Model development and analysis*; Model verification and validation; • **General and reference** → **Cross-computing tools and techniques**; *Reliability*; • **Mathematics of computing** → **Mathematical analysis**; *Numerical analysis.*

Keywords: Functional Block Diagrams, Event Trees, Safety Analysis, Theorem Proving, HOL4, Nuclear Power Plant.

ACM Reference Format:
Mohamed Abdelghany and Sofiène Tahar. 2022. Formal Probabilistic Risk Assessment of a Nuclear Power Plant. In *Proceedings of the 8th ACM SIGPLAN International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS '22), December 07, 2022, Auckland, New Zealand*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3563822.3568018

FTSCS '22, December 07, 2022, Auckland, New Zealand

ACM ISBN 978-1-4503-9907-4/22/12…$15.00
https://doi.org/10.1145/3563822.3568018

1 Introduction

1.1 Motivation

In many safety-critical complex systems, a catastrophic accident may happen due to the coincident occurrence of multiple sudden events in different subsystem components. These undesirable accidents in safety-critical systems may result in huge financial losses and sometimes severe injury or fatalities. Therefore, the central safety inquiry in many complex systems is to identify the possible consequences given that one or more sudden events could happen at a subsystem level. For that purpose, several dependability modeling techniques have been developed for safety analysis of critical-systems, such as Fault Trees (FT) [15], Reliability Block Diagrams (RBD) [22] and Event Trees (ET) [19]. FTs and RBDs are used to either analyze the factors causing a complete system failure or the complete success relationships of a system only, respectively. In contrast to FTs and RBDs, ETs provide a complete analysis for all possible complete/partial failure and success consequence scenarios that can occur in a system. Moreover, ET analysis can be used to associate failure and success events to all subsystems of a safety-critical system in more complex hierarchical structures, such as Functional Block Diagrams (FBD) [11]. An FBD is a graphical representation of the detailed system functionality and the functional relationship between all its subsystems that are represented as Functional Blocks (FB). Each FB describes the failure characteristics of a subsystem by modeling its component failure and success relationship in terms of an ET structure [19]. All these subsystem level ETs associated with their corresponding FBs are then composed together to build a complete subsystem-level ET model of a complex system. In this paper, we propose to conduct the formal probabilistic analysis of a nuclear power plant modeled in terms of FBDs.

1.2 Literature Review

We recently developed, in [2], a comprehensive library (theory) in the HOL4 theorem prover [21] for ET analysis, which allowed us to perform the formal probabilistic risk assessment for any given system consisting of N components at the system level [5]. Based on that ET library, we performed, in [3], the formal system-level reliability analysis of a Microgrid system incorporating distributed renewable energy generation systems. Moreover, in [4], we proposed a combined library of ETs and FTs analysis techniques in HOL4

for large scale *n-level* cause consequence failure analysis of power networks at the subsystem generation level. A limitation of the above work is that we can only assign two states to each subsystem, i.e., YES (success) and NO (failure). If planners/designers need to assign multi-state of complete/partial failure and reliability to each subsystem during the reliability analysis of realistic systems, then we need a hierarchical graph structure based on ETs, such as Functional Block Diagrams (FBD), for the probabilistic risk assessment.

Papazoglou [11] was the only researcher to lay down the probabilistic risk analysis of a nuclear power plant using FBDs, where the analysis is done purely manually using a paper-and-pencil approach. Following the recommendations of safety standards, such as IEC 61850 [16], EN 50128 [8], and ISO 26262 [17], we have formalized, in [1], the FBD mathematical foundations in HOL4 in order to enable the formal analysis of multi-state subsystem components and obtain all possible consequence classes (e.g., partial failure, partial success, etc.) that can occur in the whole system at the subsystem level [1]. The proposed formalization in HOL4 defines a basic FBD constructor *Functional Block* (FB), which can be used to build the mathematical expressions of *n-level* FBDs based on *multi-state* subsystem components [1].

1.3 Contributions and Paper Organization

In this paper, we conduct the FBD-based safety analysis of a nuclear power plant generation system using formal methods. In particular, we use the HOL4 theorem prover to formally verify the probabilistic expressions at the subsystem-level for all the nuclear Boiling Water Reactor (BWR) safety outcome classes of accident events that can occur in the nuclear reactor. Subsequently, in order to validate our formally verified probabilistic risk assessment results, we compare our formal analysis results with those obtained analytically and by simulation using existing techniques and tools for risk assessment. To the best of our knowledge, this is the first work that uses formal methods for the probabilistic risk assessment of a nuclear BWR. Moreover, conducted experimental results showed the superiority of our approach in terms of scalability, expressiveness, accuracy and CPU time.

The rest of the paper is organized as follows: Section 2 introduces the preliminaries for the reader to understand the rest of the paper. In Section 3, we present the formal FBD-based safety analysis of the nuclear power plant. Lastly, Section 4 concludes the paper.

2 Preliminaries

2.1 Functional Block Diagrams

Functional Block Diagrams (FBDs) are a probabilistic risk assessment technique that can construct hierarchical ET structures to perform subsystem-level reliability analysis for complex systems. A Functional Block (FB) is the basic constructing element of an FBD graph that represents the stochastic behavior of each subsystem in a safety-critical system. To present a clear understanding of FBD-based safety analysis, consider a turbine governor system of a steam power plant that controls the position of a steam inlet valve (V), which in turn regulates the steam flow to the turbine and thus controls the output power. The valve operates with an induction motor (IM) that is energized by a power supply (PS), as shown in Fig. 1. The main objective of the valve is to control the Steam Flow (SF) at point B given the flow situation at point A and a command signal C that dictates the required function of the valve, i.e. open or close. The FBD *six* step-wise analysis, defined by Papazoglou [11], are as:

1. *FBD Construction*: A system FBD (decomposed into FBs) is constructed based on the engineering knowledge to describe the subsystem-level behavior, as shown in Fig. 2.
2. *ET Generation*: Construct a complete ET model corresponding to each subsystem FB. Assuming each subsystem component is represented by two operating states only, i..e, Success (S) or Fail (F). Fig. 3 depicts the subsystem complete ETs, i.e., $ET_{1(Complete)}$, $ET_{2(Complete)}$ and $ET_{3(Complete)}$ corresponding to FB_1, FB_2 and FB_3, respectively, of the steam-turbine governor.
3. *ET Composition*: All ETs associated with their corresponding FBs are composed together considering the functional behavior of the governor system to form a complete subsystem-level ET model. For instance, $ET_{1(Complete)}$, $ET_{2(Complete)}$ and $ET_{3(Complete)}$ are composed to form the subsystem-level $ET_{Governor}$, as shown in Fig 3, with all possible complete/partial failure and reliability ET consequence paths that can occur.
4. *Probabilistic Analysis*: Lastly, evaluate the probabilities of the system complete ET paths based on the occurrence of a certain event. These probabilities represent the likelihood of each unique sequence at the component-level that is possible to occur in a system so that *only one* can occur. For example, the probability of IM Complete Failure (CF) and Governor Complete Success (CS) shown in Fig 3, i.e., $\sum_{probability(Paths\ 4-31)}$

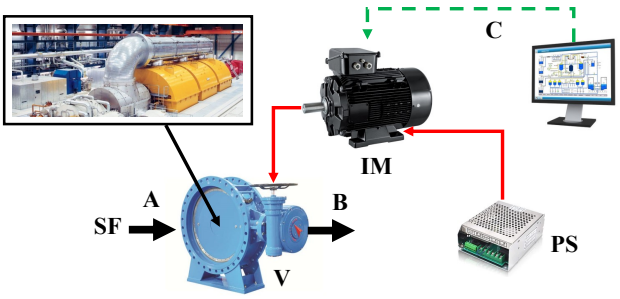

Figure 1. Steam-Turbine Governor of a Power Plant

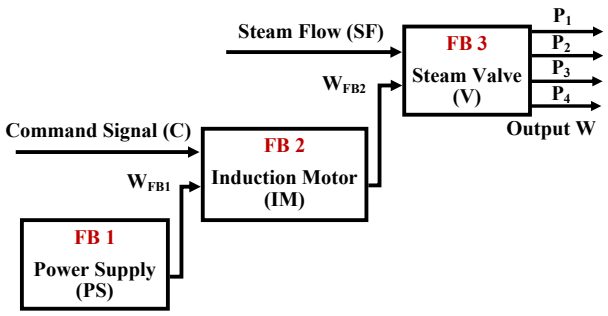

Figure 2. FBD of Steam-Turbine Governor

and Path_0, respectively, can be expressed mathematically after shorthand as:

$$\begin{aligned} Pr(\text{IM}_{CF}) &= Pr(\text{PS}_S) \times Pr(\text{C}_S) \times Pr(\text{IM}_F) + \\ &\quad Pr(\text{PS}_S) \times Pr(\text{C}_F) \; + \; Pr(\text{PS}_F) \\ Pr(\text{Governor}_{CS}) &= Pr(\text{PS}_S) \times Pr(\text{C}_S) \times Pr(\text{IM}_S) \times \\ &\quad Pr(\text{SF}_S) \times Pr(\text{V}_S) \end{aligned} \tag{1}$$

where $Pr(X_F)$ is the probability of failure for a component X and $Pr(X_S)$ represents the correct functioning of the component, i.e., 1 - $Pr(X_F)$.

2.2 FBD Library in HOL4

In [1], we have developed a HOL4 library (theory) for the the formal modeling and analysis of FBDs using theorem proving. For instance, we formalized the notion of FBDs by defining a modeling function for its basic element FB, in HOL4 as follows:

Definition 1: *Functional Block*

$\vdash \mathcal{FB}\ (\mathcal{S}::\mathcal{I}_N) = \mathcal{I}_N \bigotimes_{\text{L}}^{N} \mathcal{S}$

where the function $\bigotimes_{\text{L}}^{N}$ takes two input lists and generates a corresponding complete ET mathematical model. $\mathcal{S}$ is a list of all subsystem internal components failure and success states and $\mathcal{I}_N$ is a *two-dimensional* list of all inputs states that affect the subsystem FB, i.e., $\mathcal{I}_N$ = [[I_1]; [I_2]; [I_3];...; [I_n]]. Also, we can obtain the ET model of a specific functional block $\mathcal{FB}_j$ by defining a function $\mathcal{FB}_{ET}$, in HOL4 as follows:

Definition 2: *Functional Block ET*

$\vdash \mathcal{FB}_{ET}\ \mathcal{FB}_j$ = ETREE (NODE $\mathcal{FB}_j$)

To construct multiple consecutive N FBs, we define the following recursive function $\mathcal{FB}_{ET}^{N}$, in HOL4 as follows:

Definition 3: *Multiple Functional Block ET*

$\vdash \mathcal{FB}_{ET}^{N}\ (\mathcal{FB}_1::\mathcal{FB}_N) = \mathcal{FB}_{ET}\ \mathcal{FB}_1::\mathcal{FB}_{ET}^{N}\ \mathcal{FB}_N$

Then, we defined a *three-dimensional* function $\mathcal{FB}_N$ that takes N FBs, where each FB takes an arbitrary list of n-inputs and then generates the corresponding complete FBD model to obtain all possible risk consequences of failure and reliability, in HOL4 as:

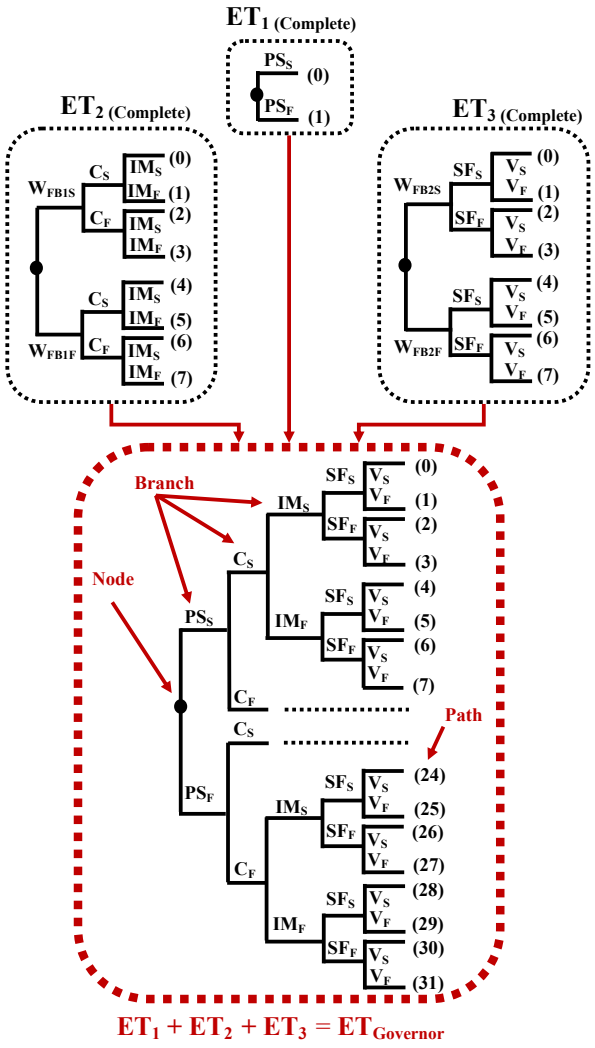

Figure 3. Steam-Turbine Governor ET Diagrams

Definition 4: *Three Dimensional N Functional Blocks*

$\vdash \mathcal{FB}_N\ (\mathcal{SI}_1::\mathcal{SI}_2::\mathcal{SI}_N) =$
$\mathcal{FB}$ (MAP (λa. $\mathcal{FB}$ a) ($\mathcal{SI}_1::\mathcal{SI}_2::\mathcal{SI}_N$))

The prime purpose of the above-mentioned formalization of FBDs is to build a reasoning support for the subsystem-level formal safety analysis of realistic complex systems within the sound environment of HOL4. In the next section, we present the formal FBD-based safety analysis of a nuclear power plant generation system to illustrate the applicability of our proposed formal approach.

3 Nuclear Power Plant System

An electrical power system consists of three major sectors [13]: (i) generating power stations; (ii) transmission lines; and (iii) distribution grids. A Nuclear Power Plant [20] is a thermal generating station that has the capability to produce 24,000 MWh per 1 kg uranium [6]. For that reason, it is widely

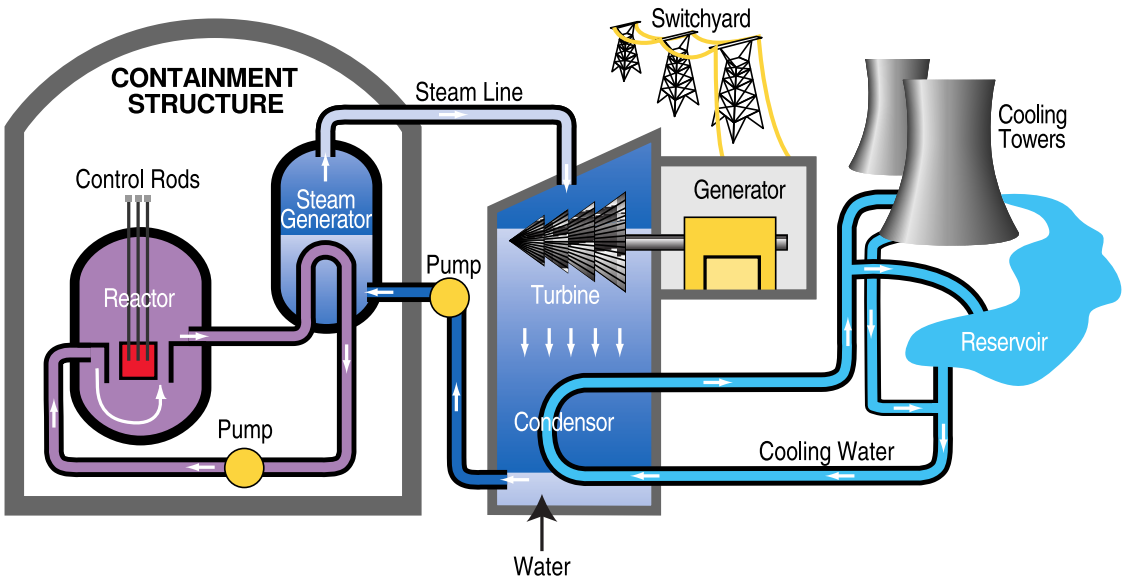

Figure 4. Nuclear Power Plant Structure [9]

used by developing countries to satisfy the rapid increase in customers' demands. However, nuclear power installations are vulnerable to accidents causing the contamination with radioactive material, which would make a large surrounding area uninhabitable for thousands of years. Therefore, there is a dire need to develop safety analysis techniques for nuclear power plants making them more safe to radioactive disasters and enable back-up decisions [7]. Inside the nuclear power station, the conversion to electrical energy takes place similar to other thermal power stations, as shown in Fig. 4 [9]. First, the nuclear reactor heats the reactor coolant, which could be water or gas, based on the reactor's type. Then, the reactor coolant passes to a steam generator, which heats water and produces a steam flow. The pressurized steam flow then goes to a steam turbine, which starts to produce power and the remaining vapor is condensed through a condenser. The condenser is used to exchange heat through a secondary side, for instance, a river or a cooling tower. The condensed water is again pumped back to the steam generator and the cycle repeats. In the sequel, we use our formalization of FBDs to analyze in HOL4 the probabilities of all possible classes of accident events that can occur in the nuclear reactor.

3.1 Formal FBD Modeling

Fig. 5 [11] depicts the system-level FBD of a nuclear Boiling Water Reactor (BWR) that could have one of the following Initial Events (IE) [14]: (a) *L*: Large loss of coolant accident; (b) *M*: Medium loss of coolant accident; and (c) *S*: Small loss of coolant accident; and (d) *T*: Transient accident. Based on these IEs, there are *four* classes of accidents that can occur, as shown in Fig. 5: (1) *CLASS I*: Containment intact when the nuclear reactor core melts at low pressure; (2) *CLASS II*: Containment failing when the nuclear reactor core melts; (3) *CLASS III*: Containment intact when the nuclear reactor core melts at high internal pressure; and (4) *CLASS IV*: Containment failing prior to the nuclear reactor core melting due to severe overpressure. The characteristic of each class is based on the melting time of the reactor's core, i.e., before or after the containment, as well as the pressure status when the containment fails. All these parameters affect the extent of the consequences of the radioactivity released in the surrounding environment. The system-level FBD analysis of the BWR system for safety of the nuclear power plant can be formally modeled, in HOL4 as:

Definition 5:

```
⊢ System_Level_FBD_BWR [[L;M;S;T];[S_BWR]]
  [P_SUCCESS;P_CLASS_I;P_CLASS_II;P_CLASS_III;P_CLASS_IV] =
  FB_ET [⊞ P_SUCCESS (FB [[L;M;S;T];[S_BWR]]);
         ⊞ P_CLASS_I  (FB [[L;M;S;T];[S_BWR]]);
         ⊞ P_CLASS_II (FB [[L;M;S;T];[S_BWR]]);
         ⊞ P_CLASS_III (FB [[L;M;S;T];[S_BWR]]);
         ⊞ P_CLASS_IV (FB [[L;M;S;T];[S_BWR]])]
```

where the function ⊞ takes the function $\mathcal{FB}$ and a partitioning event list P corresponding to a certain reliability events

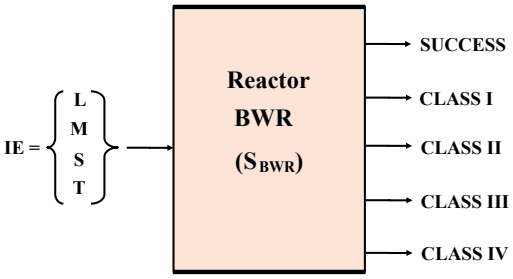

Figure 5. System-Level FBD of BWR

and outcomes the corresponding ET model, as described in [2]. To study the internal states of the reactor S_{BWR} hierarchically, the system-level FBD is decomposed into 3 major *first-level* FBs (Fig. 6) as [11]:

(1) *Reactivity Control* (FB_1): It stops the chain reaction of the reactor. It is mainly controlled by the insertion of control rods, as shown in Fig. 4. It has two internal states: (a) C_1 represents that the reactivity is successfully controlled; and (b) C_2 represents that the reactivity cannot be controlled.
(2) *Reactor Coolant Inventory Control* (FB_2): It provides the reactor core with an adequate amount of coolant to maintain its necessary inventory. Two internal states are considered: (a) R_1 represents the successful functioning of the reactor coolant inventory control; and (b) R_2 the failure of the reactor coolant inventory control.
(3) *Decay Heat Removal* (FB_3): It removes the decay and the stored heat from the reactor core to the environment. It considers two internal states: (a) H_1 represents that the function of decay heat removal can be done successfully; and (b) H_2 represents the failure of decay heat removal.

We can formally define the decomposed *first-level* FBD model of the BWR system, as shown in Fig. 6, in HOL4 as:

Definition 6:

```
⊢ Let W_C1' = ⊞ P_C1' (FB [[L;M;S;T];[C1;C2]])
  in
  FIRST_LEVEL_FBD_BWR
  [[L;M;S;T];[C1;C2];[R1;R2];[H1;H2]]
  [P_C1';P_C2';P_R1';P_R2';P_R3';P_H1';P_H2'] =
  FB_ET [⊞ P_C2' (FB [[L;M;S;T];[C1;C2]]);
         ⊞ P_R2' (FB [W_C1';[R1;R2]]);
         ⊞ P_R3' (FB [W_C1';[R1;R2]]);
         ⊞ P_H2' (FB [⊞ P_R1'
                      (FB [W_C1';[R1;R2]]);[H1;H2]]);
         ⊞ P_H1' (FB [⊞ P_R1'
                      (FB [W_C1';[R1;R2]]);[H1;H2]])]
```

Now, we can decompose the *first-level* FBD of BWR to *multiple-levels* describing the details of BWR safety functions, as shown in Fig. 7 [11] to obtain a complete 6,144 possible test cases (4×2×3×2×2×2×2×2×2×2×2). The decomposed

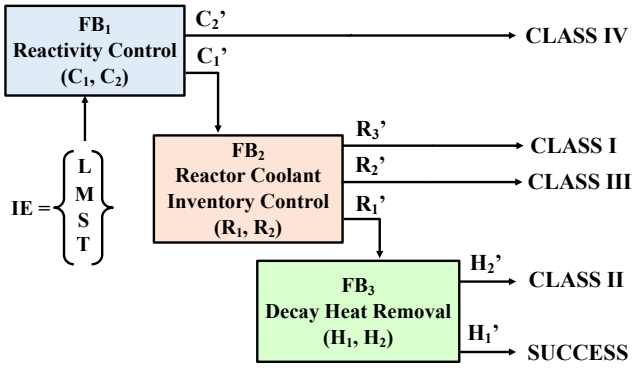

Figure 6. First-Level FBD of BWR

FBD is constructed based on the nuclear power engineering knowledge to describe the system behavior, which can be summarized as follows [11]:

(1) The process to control the reactor coolant inventory of BWR can be performed either at high or low pressure. The first priority is to do the control process at high pressure (FB_{21}), but if it is not available, then the process should be performed at low pressure (FB_{23}) through a depressurization of the reactor coolant circuit (FB_{22}), as shown in Fig. 7.
(2) The integrity of the high-pressure reactor coolant inventory (FB_{21}) can be preserved through using either a feed-water Power Conversion System (PCS) (FB_{212}) or High Pressure Core Injection (HPCI) and Reactor Core Isolation Cooling (RCIC) (FB_{213}). This is done after the water relief operation (FB_{211}), which opens safety valves enough for relieving the pressure from the circuit. The failure to relieve the pressure will lead to an undesirable break.
(3) The low pressure reactor coolant inventory control (FB_{23}) is decomposed into three safety functions: (a) Low Pressure Coolant Injection (FB_{231}); (b) Emergency Coolant Injection (FB_{232}); and (c) Coolant Recirculation (FB_{233}).
(4) Finally, the decay heat (FB_3) is removed from the reactor core using: (a) Direct Power Conversion (DPC) (FB_{31}); and (b) Residual Heat Removal (RHR) (FB_{32}), which transfer the decay heat to a heat-sink in the power station.

Each FB of the BWR can be assigned with a multi-state model for safety analysis, as shown in Fig. 8 [7]. Assuming that each FB has two possible safety states only (correct functioning X_1 and failure operation X_2). Since the pressure relief process (FB_{211}) is a very critical process, therefore, it is represented by 3-state model (see Fig. 8): (a) Y_1: Safety valve functions correctly for pressure relief (opens and then recloses); (b) Y_2: Safety valve fails to open; and (c) Y_3: Safety valve functions partly properly (opens but fails to recloses), as shown in Fig. 7. Based on the above detailed description of the decomposed *multiple-levels* FBD of the nuclear power plant

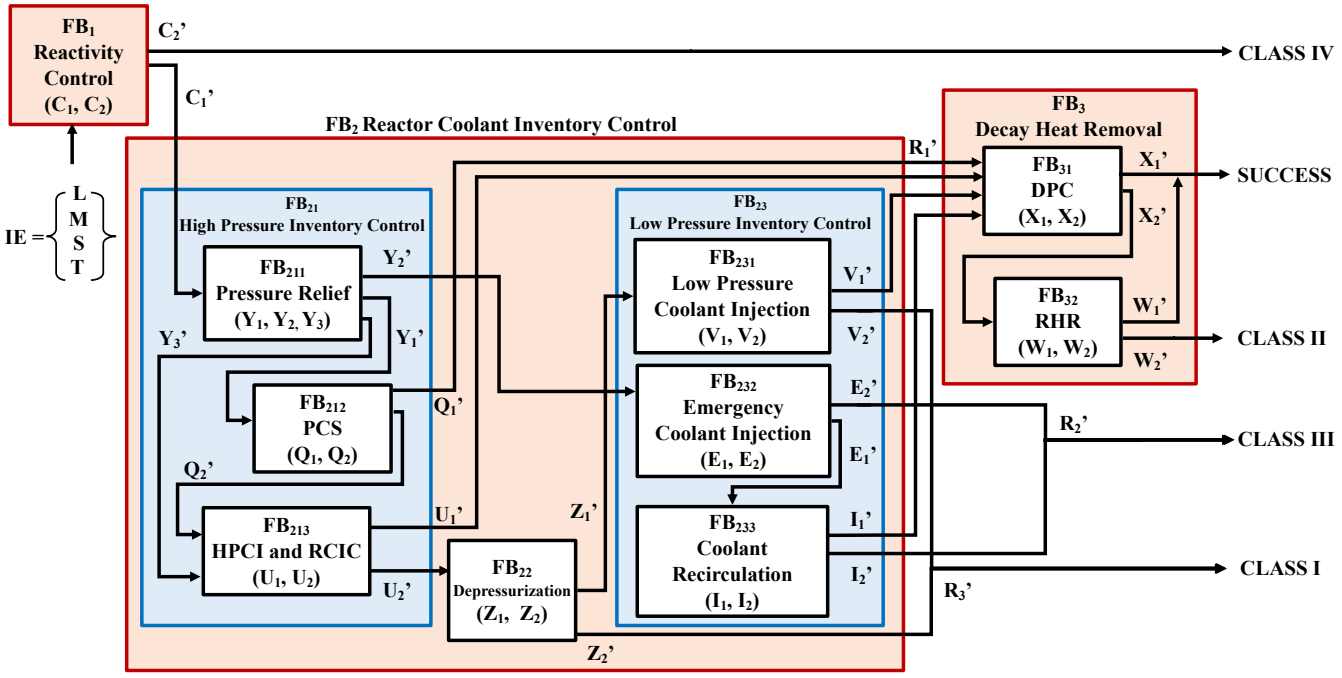

Figure 7. FBD Multiple-Levels Decomposition of BWR

system, we can formally define its graphical FBD, as shown in Fig. 7, associated with all the safety classes, in HOL4 as:

Definition 7:

```
⊢ Let
  W_C1' = FB  [[L;M;S;T];[C1]];
  W_C2' = FB  [[L;M;S;T];[C2]];
  W_Q1' = FB_N [W_C1';[Y1];[Q1]];
  W_U1' = FB_N [[W_C1';[Y1];[Q2]];
                [W_C1';[Y3]];[U1]];
  W_Z2' = FB_N [[W_C1';[Y1];[Q2]];
                [W_C1';[Y3]];[U2];[Z2]];
  W_V1' = FB_N [[W_C1';[Y1];[Q2]];
                [W_C1';[Y3]];[U2];[Z1];[V1]];
  W_V2' = FB_N [[W_C1';[Y1];[Q2]];
                [W_C1';[Y3]];[U2];[Z1];[V2]];
  W_E2' = FB_N [W_C1';[Y2];[E2]];
  W_I1' = FB_N [W_C1';[Y2];[E1];[I1]];
  W_I2' = FB_N [W_C1';[Y2];[E1];[I2]];
  W_X1' = FB_N [W_Q1';W_U1';W_V1';W_I1';[X1]];
  W_W1' = FB_N [W_Q1';W_U1';W_V1';W_I1';[X2];[W1]];
  W_W2' = FB_N [W_Q1';W_U1';W_V1';W_I1';[X2];[W2]];
  L_IEs    = [L ↓ ; M ↓; S ↓; T ↓]
  L_States = [[C1 ↑; C2 ↓]; [Y1 ↑; Y2 ↓; Y3 ↓];
              [Q1 ↑; Q2 ↓]; [U1 ↑; U2 ↓];
              [Z1 ↑; Z2 ↓]; [V1 ↑; V2 ↓];
              [E1 ↑; E2 ↓]; [I1 ↑; I2 ↓];
              [X1 ↑; X2 ↓]; [W1 ↑; W2 ↓]]
  in
  OUTCOME_CLASS_I_BWR L_IEs L_States =
```

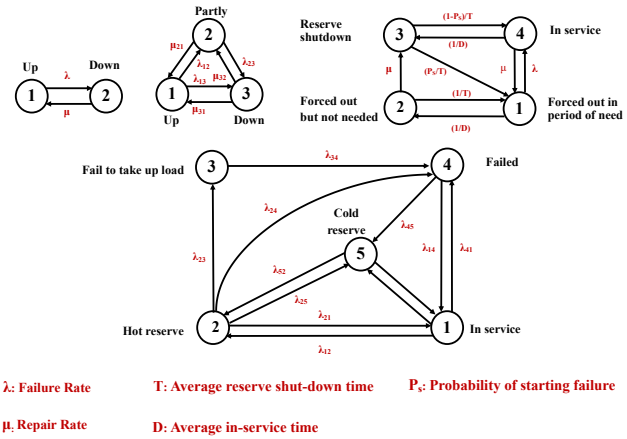

Figure 8. Multi-State Models for Safety Studies

```
FB_ET (FB_ET^N [W_V2';W_Z2'])
OUTCOME_CLASS_II_BWR L_IEs L_States =
FB_ET (W_W2')
OUTCOME_CLASS_III_BWR L_IEs L_States =
FB_ET (FB_ET^N [W_E2';W_I2'])
OUTCOME_CLASS_IV_BWR L_IEs L_States =
FB_ET (W_C2')
OUTCOME_SUCCESS_BWR L_IEs L_States =
FB_ET (FB_ET^N [W_X1';W_W1'])
```

where the failure function ↓ or Cumulative Distribution Function (CDF) takes a component X and returns a set of all the

values less or equal to time t, i.e., $X \leq t$, while the success function $\uparrow$ is the complement of the function $\downarrow$, i.e, $X > t$.

3.2 Formal FBD Probabilistic Analysis

Using our proposed ET and FBD probabilistic theorems and under their constraints, we can *formally verify* the probabilistic expression at the subsystem-level for any of the BWR safety outcome classes that could occur in the nuclear power plant. We assume that the failure and success events of all components within the nuclear power plant system are exponentially distributed, which is well-known as *memoryless* and is routinely used in the reliability analysis of realistic systems, i.e., `X ↓ = 1 - e^(-λX t)` and `X ↑ = e^(-λX t)`, where λ_X is the failure rate of the component X and t is a time index. For the numerical results, we assume that the reliability study is undertaken for one year only, i.e., t = 8760 hours (24 hours × 365 days), so that the summation of failure and success probabilities for each component is equals to one. Therefore, we can verify the probabilistic mathematical expressions of all safety outcome classes at the subsystem-level for the nuclear power plant, respectively, in HOL4 as:

Theorem 1: *Containment Failing when BWR Core Melts*

$$
\begin{aligned}
&\vdash \Omega_C^N\ [\mathtt{L};\mathtt{M};\mathtt{S};\mathtt{T}] \Rightarrow \\
&\quad \mathtt{prob\ p\ (OUTCOME\_CLASS\_II\_BWR\ L_{IEs}\ L_{States})} = \\
&(1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times e^{(-\lambda_Q t)} \times \\
&(1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + (1-e^{(-\lambda_M t)}) \times e^{(-\lambda_C t)} \times \\
&e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times e^{(-\lambda_Q t)} \times (1-e^{(-\lambda_X t)}) \times \\
&(1-e^{(-\lambda_W t)}) + (1-e^{(-\lambda_S t)}) \times e^{(-\lambda_C t)} \times e^{(-\lambda_{Y2} t)} \times \\
&e^{(-\lambda_{Y3} t)} \times e^{(-\lambda_Q t)} \times (1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + \\
&(1-e^{(-\lambda_T t)}) \times e^{(-\lambda_C t)} \times e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times e^{(-\lambda_Q t)} \times \\
&(1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + (1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times \\
&e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times (1-e^{(-\lambda_Q t)}) \times e^{(-\lambda_U t)} \times \\
&(1-e^{(-\lambda_X t)}) \times \ldots \times \ldots \\
&+ \ldots + \ldots + \ldots + \\
&(1-e^{(-\lambda_M t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y3} t)}) \times e^{(-\lambda_U t)} \times \\
&(1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + \ldots + (1-e^{(-\lambda_S t)}) \times \\
&e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y3} t)}) \times (1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times \\
&e^{(-\lambda_V t)} \times \ldots \times \ldots + \ldots + \ldots + \ldots
\end{aligned}
$$

where the function Ω_C^N ensures that all multi-state events are *distinct* (not similar to each other) and *disjoint* (cannot occur at the same time), as described in [2].

Theorem 2: *Containment Intact at High Internal Pressure*

$$
\begin{aligned}
&\vdash \Omega_C^N\ [\mathtt{L};\mathtt{M};\mathtt{S};\mathtt{T}] \Rightarrow \\
&\quad \mathtt{prob\ p\ (OUTCOME\_CLASS\_III\_BWR\ L_{IEs}\ L_{States})} = \\
&(1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times (1-e^{(-\lambda_E t)}) + \\
&(1-e^{(-\lambda_M t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times (1-e^{(-\lambda_E t)}) + \\
&(1-e^{(-\lambda_S t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times (1-e^{(-\lambda_E t)}) + \\
&(1-e^{(-\lambda_T t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times (1-e^{(-\lambda_E t)}) + \\
&(1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times e^{(-\lambda_E t)} \times \\
&(1-e^{(-\lambda_I t)}) + \ldots + \ldots + (1-e^{(-\lambda_T t)}) \times e^{(-\lambda_C t)} \times \\
&(1-e^{(-\lambda_{Y2} t)}) \times e^{(-\lambda_E t)} \times (1-e^{(-\lambda_I t)})
\end{aligned}
$$

Theorem 3: *Containment Intact at Low Pressure*

$$
\begin{aligned}
&\vdash \Omega_C^N\ [\mathtt{L};\mathtt{M};\mathtt{S};\mathtt{T}] \Rightarrow \\
&\quad \mathtt{prob\ p\ (OUTCOME\_CLASS\_I\_BWR\ L_{IEs}\ L_{States})} = \\
&(1-e^{(-\lambda_L t)}) \times (1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times (1-e^{(-\lambda_V t)}) \times \\
&(1-e^{(-\lambda_Q t)}) \times e^{(-\lambda_{Y2} t)} \times \ldots + \ldots + (1-e^{(-\lambda_S t)}) + \\
&(1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times (1-e^{(-\lambda_V t)}) \times (1-e^{(-\lambda_Q t)}) \times \\
&e^{(-\lambda_{Y2} t)} \times \ldots + \ldots + \ldots + (1-e^{(-\lambda_M t)}) \times \\
&(1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times (1-e^{(-\lambda_V t)}) \times (1-e^{(-\lambda_{Y3} t)}) \times \\
&e^{(-\lambda_C t)} + \ldots + \ldots + (1-e^{(-\lambda_T t)}) \times (1-e^{(-\lambda_U t)}) \times \\
&(1-e^{(-\lambda_Z t)}) \times (1-e^{(-\lambda_{Y3} t)}) \times e^{(-\lambda_C t)}
\end{aligned}
$$

Theorem 4: *BWR of Power Plant Functions Correctly*

$$
\begin{aligned}
&\vdash \Omega_C^N\ [\mathtt{L};\mathtt{M};\mathtt{S};\mathtt{T}] \Rightarrow \\
&\quad \mathtt{prob\ p\ (OUTCOME\_SUCCESS\_BWR\ L_{IEs}\ L_{States})} = \\
&1 - \Big(\\
&(1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times e^{(-\lambda_Q t)} \times \\
&(1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + \ldots + (1-e^{(-\lambda_M t)}) \times \\
&e^{(-\lambda_C t)} \times e^{(-\lambda_{Y2} t)} \times e^{(-\lambda_{Y3} t)} \times (1-e^{(-\lambda_Q t)}) \times e^{(-\lambda_U t)} \times \\
&(1-e^{(-\lambda_X t)}) \times \ldots + \ldots + (1-e^{(-\lambda_S t)}) \times e^{(-\lambda_C t)} \times \\
&(1-e^{(-\lambda_{Y3} t)}) \times e^{(-\lambda_U t)} \times (1-e^{(-\lambda_X t)}) \times (1-e^{(-\lambda_W t)}) + \\
&\ldots + (1-e^{(-\lambda_L t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y3} t)}) \times \\
&(1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times e^{(-\lambda_V t)} \times \ldots + \ldots + \ldots + \\
&(1-e^{(-\lambda_T t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times (1-e^{(-\lambda_E t)}) + \\
&\ldots + (1-e^{(-\lambda_M t)}) \times e^{(-\lambda_C t)} \times (1-e^{(-\lambda_{Y2} t)}) \times e^{(-\lambda_E t)} \times \\
&(1-e^{(-\lambda_I t)}) + \ldots + \ldots + (1-e^{(-\lambda_L t)}) \times (1-e^{(-\lambda_U t)}) \times \\
&e^{(-\lambda_Z t)} \times (1-e^{(-\lambda_V t)}) \times (1-e^{(-\lambda_Q t)}) \times e^{(-\lambda_{Y2} t)} \times \ldots + \\
&(1-e^{(-\lambda_S t)}) \times (1-e^{(-\lambda_U t)}) \times e^{(-\lambda_Z t)} \times (1-e^{(-\lambda_V t)}) \times \\
&\ldots + \ldots + \ldots \Big)
\end{aligned}
$$

In order to validate our formally verified results and compare their accuracy with other main stream reliability approaches, we have developed Standard Meta Language (SML) functions to numerically compute the verified probabilistic expressions at the subsystem level. In the sequel, we compare our formal analysis results with those obtained using: (1) manual paper-and-pencil analysis we conducted the following the FBD step-wise assessment proposed in [11]; (2) the commercial Isograph software for ET analysis [12]; and (3) MATLAB Monte-Carlo Simulation (MCS) following the random-based algorithm proposed in [18]. The objective of the experiment is to compare the different approaches from the modeling effort and computation point of views. The MCS randomly predicts the real behavior patterns to estimate the average value of the various safety classes of complete/partial failure and reliability. On the other hand, Isograph does not analyze FBDs directly but rather ET models only, and hence the FBD of the BRW (Fig. 7) had to be converted to a flat network of ETs. We consider the failure rates of the nuclear power plant components λ_L, λ_M, λ_S, λ_T, λ_C, λ_{Y2}, λ_{Y3}, λ_Q, λ_W, λ_U, λ_Z, λ_V, λ_E, λ_X, λ_I to be, respectively, 0.11, 0.12, 0.15, 0.16, 0.21, 0.15, 0.21, 0.57, 0.42, 0.23, 0.22, 0.16, 0.12, 0.57, and 0.46 per year [10]. Table 1 summarizes the computed SML, manual, Isograph and MATLAB results for all outcome classes.

It can be noticed that the results of safety classes obtained from our formal analysis are equivalent to the corresponding ones calculated using paper-and-pencil as well as Isograph software augmented with added accuracy in the computed

Table 1. Safety Class Results of the Nuclear Power Plant

Classes	Manual	Isograph	MATLAB	HOL4
CLASS I	0.01308	0.0131	0.0195	0.01308055491
CLASS II	0.05685	0.0569	0.0628	0.05684465922
CLASS III	0.02506	0.0251	0.0303	0.02506380531
CLASS IV	0.09554	0.0955	0.0896	0.09554010593
SUCCESS	0.80947	0.8095	0.7978	0.80947082132
CPU Time (Seconds)	–	35.461	112.928	8.123

values. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results at every generation of a random number with errors between 3-8%. Moreover, the total CPU time for the above safety classes analysis using the SML functions is much faster than Isograph (4X) and MATLAB MCS (14X), as shown in Table 1. The experiments were performed on core i5, 2.20 GHz processor, running under Linux VM with 1 GB of RAM. It required several days to model the nuclear power plant using the manual analysis while it was less time consuming (a matter of hours) using the Isograph software and MATLAB MCS, but the least modeling time is through using the HOL4 theorem prover. This clearly elucidates that our multi-level analysis of multi-state events is not only providing the correct results but also *formally proven* probabilistic expressions (Theorems 1-4) compared to all existing techniques. Therefore, we are providing the *first formal mechanical analysis* of FBDs ever, augmented with the rigor of HOL theorem proving for accurate subsystem-level safety evaluation. Moreover, our proposed formalization is capable of enabling the *verification* of all possible safety classes of complete/partial failure of critical systems of any size and compute their reliability events simultaneously. For instance, our FBD formalization framework can handle a realistic nuclear power plant generation system consisting of *multi-level* decomposition subsystems, where each subsystem is composed of M components and each component is associated with *multi-state* failure and success consequence events.

4 Conclusions

We used a novel methodology based on formal techniques to conduct a multi-state probabilistic risk assessment of a safety-critical nuclear power plant system. Using the HOL4 theorem prover, we accurately verified its probabilistic expressions for all possible risk consequence classes that can occur at the subsystem level. Moreover, we evaluated the formally verified probabilistic expressions of BWR safety classes using SML functions and compared them to existing informal approaches of MATLAB Monte-Carlo random-based algorithms, the Isograph ET analysis tool and manual paper-and-pencil mathematical analysis. We believe that our work will help safety design engineers to meet the desired quality requirements. As future work, we plan to develop an integrated framework with a GUI for FBD modeling and linking ET tools with the FBD formalization in HOL4.

References

[1] M. Abdelghany. 2021. Formal Probabilistic Risk Assessment using Theorem Proving with Applications in Power Systems, PhD thesis, Concordia university, Montreal, QC, Canada.

[2] M. Abdelghany, W. Ahmad, and S. Tahar. 2022. Event Tree Reliability Analysis of Safety-Critical Systems Using Theorem Proving. *IEEE Systems Journal* 16, 2 (2022), 2899–2910.

[3] M. Abdelghany and S. Tahar. 2020. Event Tree Reliability Analysis of Electrical Power Generation Network using Formal Techniques. In *Electric Power and Energy Conference*. IEEE, 1–7.

[4] M. Abdelghany and S. Tahar. 2021. Cause-Consequence Diagram Reliability Analysis Using Formal Techniques With Application to Electrical Power Networks. *IEEE Access* 9 (2021), 23929–23943.

[5] M. Abdelghany and S. Tahar. 2022. Reliability Analysis of Smart Grids Using Formal Methods. In *Handbook of Smart Energy Systems*. Springer, 1–17. https://doi.org/10.1007/978-3-030-72322-4_81-1

[6] S. Ahmed. 2019. The Impact of Emergency Operating Safety Procedures on Mitigation the Nuclear Thermal Power Plant Severe Accident. *Annals of Nuclear Energy* 125 (2019), 222–230.

[7] R. N. Allan. 2013. *Reliability Evaluation of Power Systems*. Springer Science & Business Media.

[8] J. L. Boulanger. 2015. *CENELEC 50128 and IEC 62279 Standards*. John Wiley & Sons.

[9] M. Čepin. 2011. *Assessment of Power System Reliability: Methods and Applications*. Springer Sci. & Bus. Media.

[10] J. Choi and H. Seok. 2020. Development of Risk Assessment Framework and the Case Study for a Spent Fuel Pool of a Nuclear Power Plant. *Nuclear Engineering and Technology* (2020).

[11] I. Papazoglou. 1998. Functional Block Diagrams and Automated Construction of Event Trees. *Reliability Engineering & System Safety* 61, 3 (1998), 185–214.

[12] Isograph. 2022. https://www.isograph.com

[13] R. Karki, R. Billinton, and A. K. Verma. 2014. *Reliability Modeling and Analysis of Smart Power Systems*. Springer Science & Business Media.

[14] J. Lee and N.J McCormick. 2011. *Risk and Safety Analysis of Nuclear Systems*. John Wiley & Sons.

[15] N. Limnios. 2013. *Fault Trees*. John Wiley & Sons.

[16] R. E. Mackiewicz. 2006. Overview of IEC 61850 and Benefits. In *Power Systems Conference and Exposition*. IEEE, 623–630.

[17] R. Palin, D. Ward, I. Habli, and R. Rivett. 2011. ISO 26262 Safety Cases: Compliance and Assurance. In *IET Conference on System Safety*. 1–6.

[18] N. Papakonstantinou, S. Sierla, B. O'Halloran, and Y. Tumer. 2013. A Simulation based Approach to Automate Event Tree Generation for Early Complex System Designs. In *Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, Vol. 55867. American Society of Mechanical Engineers, 1–10.

[19] I. Papazoglou. 1998. Mathematical Foundations of Event Trees. *Reliability Engineering & System Safety* 61, 3 (1998), 169–183.

[20] D. E. Peplow, C. D. Sulfredge, R. L. Sanders, R. H. Morris, and T. A. Hann. 2004. Calculating Nuclear Power Plant Vulnerability Using Integrated Geometry and Event/Fault-Tree Models. *Nuclear Science and Engineering* 146, 1 (2004), 71–87.

[21] HOL4 Theorem Prover. 2022. https://hol-theorem-prover.org

[22] K. Trivedi and A. Bobbio. 2017. Reliability Block Diagrams. In *Reliability and Availability Engineering: Modeling, Analysis, and Applications*. Cambridge University Press, 105–149.

Received 2022-09-08; accepted 2022-10-10