Advances in Reliability, Safety and Security, Part 4 – Kołowrocki, Dąbrowska (eds.)
 ISBN 978-83-68136-16-6 (printed), ISBN 978-83-68136-03-6 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Modelling Reliability And Resilience Of Dual-Function Power Station

Darragi Messaoudi[a], Amr Abdellaoui[a], Dragan Komljenovic[a], Anh Chi Nguyen[b]

[a]*Hydro Quebec, Montreal, Canada*
[b]*Oxand, Lausane, Switzerland*

Abstract

The Hydro-Quebec "Beauharnois-Les Cèdres" electrical complex is a critical infrastructure whose primary mission is the water management of Saint-Lawrence River by preserving the continuity of power transmission of Beauharnois (BHN) power plant output while juggling with many other missions such as supplying local loads, exporting electricity to the state of New York, and ensuring safe operations of the whole complex. It is a system of heterogeneous systems (System of systems-SoS) with a mix of functions, technologies, and interconnections. Hence, assessing, designing, and operating a SoS using the existing power plant and adjacent power grids as a discharging means for floods will be a world first. However, it is an exceptionally large system making the problem difficult to tackle with classical reliability approaches. To address this challenge, new reliability methods were developed and applied to provide quantitative results about the SoS behavior like reliability, availability, and interesting facets of resilience such as the capacity to absorb and to adapt to extreme events. These methods are introduced through a top-down approach using a 6-level abstraction model for the overall SoS. Against this background, reliability analysis is expressed in terms of "loss of generating capacity." The purpose of this study is to explore and quantify the positive contribution of the electrical transmission system in managing flood risks.

Keywords: System of Systems (SoS), resilience, reliability, complexity, simulation, emergence

1. Introduction

When we think about BHN bordering power grid including transmission lines and substations, 4 complexity dimensions arise: (1) The extended topology, (2) multiple electric systems, (3) complex operations and (4) a water management function. All those aspects must be properly addressed:

- The topology: The Topology of the BHN generating station has a complex electrical busbar allowing a very large number of substation configurations. In fact, it consists of 36 units, 16 buses, 20 lines departures and 14 transmission lines connected to 4 independent subsystems. Thus, from system analysis perspective, it is not practical to enumerate all possible combinations.
- Adjacent Electric Systems: BHN power plant is most of the time simultaneously connected to 4 independent systems, these include the HQ system, the New York Power Authority (NYPA) system, Niagara Mohwak Power Corporation (NMPC) of National Grid (NG) and the Independent Electrical System Operator (IESO) of the province of Ontario. Within the HQ system, the BHN generating station can be connected simultaneously to three regional subsystems through seven 120 kV transmission lines.
- Operations: Since BHN power plant is most of the time simultaneously connected to 4 independent power grids, a variable number of generating units can be promptly allocated to the different adjacent systems and subsystems. This increases the operation complexity while allowing the achievement of an effective real time dispatching of the generating units. The flexibility of the BHN substation's busbar and the extensive unit dispatching possibilities require significant operational skills. For example, the post contingency spills initiated by the tripping of one or more 120 kV lines can be mitigated by performing substation reconfigurations and reconnecting the tripped units to the adjacent lines by the

operators in the control room. Thus, an experienced and skilful operator is very important to achieve a fast and effective contingency mitigation.

- A water management function: BHN generation station is a run-of-the river plant whose primary mission is the water management of the Saint-Lawrence River. The continuity of power transmission of the Beauharnois power plant output is critical for the water discharge of Beauharnois Canal and for the continuity of the maritime traffic along the St. Lawrence Seaway. A continuous monitoring of the upstream and the downstream water level is critical for a safe maritime traffic along the BHN canal. Furthermore, BHN is critical during the flood season since it is used temporarily as an "electrical spillway."

The purpose of this study is to quantify the role of the Transmission Network in the water management mission. Hence, to quantify the flow discharge capacity. It highlights all SoS critical systems (Dahmann,2015) and asset management strategies needed to secure the mission for the next 50 years. The four main objectives are to:

- simplify the electrical network through an electrical approach (Section 2);
- propose a reliability framework able to handle different SoS abstraction levels (Section 3);
- measure operations mitigation impact on the discharge capacity (Section 4);
- measure discharge capacity and the impact of power system improvements (Section 5).

2. The electrical approach

BHN generating station has a complex busbar system allowing countless possible configurations. Therefore, it's not practical to cover all possible states of the system. In the beginning, dominant operating configurations have been first identified to limit the scope of the analysis, but still preserving an adequate accuracy. Then, a contingency analysis was undertaken in terms of BHN units tripped following the loss of a single or double circuit. The goal is, on one hand, to enumerate all possible nontrivial contingencies and, on the other hand, to validate the eventual post-contingency mitigation performed by the operator using power flow simulations (Figure 1).

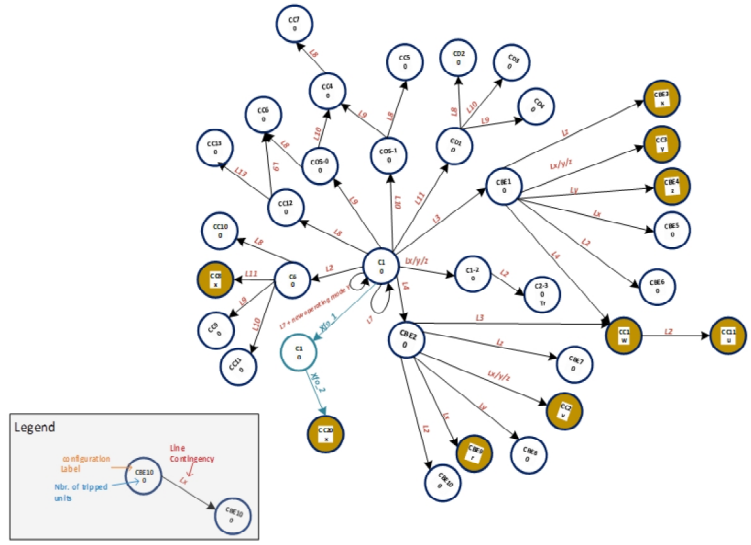

Fig. 1. Power Station Configuration (nodes) and Contingency (edges) Graph.

The philosophy of the contingency analysis approach is illustrated in Figure 1. Initially, an hourly system topology analysis is performed from the state estimator to determine the dominant configurations. Based on these results, operating experience and expected future operation, the most probable configuration (initial configuration) is defined. Optimal configurations minimizing spills were determined from the initial configuration by applying all the combinations of single and double contingencies. Those grid configurations have been used as a basis for the reliability assessment.

3. The reliability modelling approach

A multi-level solution was developed to meet the objectives of the main question, regarding the discharge capacity (Komljenovic et al., 2019). All models were integrated to communicate with each other (Figure 2). Here is a brief description of the different levels:

- Failure/Reliability Database: It is the level that captures failures with unavailability consequences on assets. They can be lethal or reparable failures. It consists of thousands of asset life curves and maintainability distributions (Exponential, Weibull, Lognormal, …).
- Asset: At this level assets are modelled as systems using FTA and RBD to include maintenance strategies or CCFs at the asset-level.
- Transmission Network: At this level power systems are modelled using FTA and RBD to include CCFs at the system level. All asset models of the previous level are already sub-diagram at this system-level.
- Virtual Operator: The operator actions are important for the system to recover from failures. He is also responsible for reducing generating units' losses and, hence minimizing spills. Thus, at this level, a new inductive and quantitative reliability method was developed to capture operator switching sequences. The output is expressed as a probabilistic distribution of the number of tripped units.
- Orchestrator: This level handles system dynamics about reconfigurations and operations processes. The right operator actions are initiated according to each specific system failed state. From the outside, it acts as a Rule Engine. From the inside, it consists of a logical model of the system disjoint states and their corresponding operator actions, all of which as probabilistic distributions in a Monte-Carlo Simulation Framework.
- Hydraulic System: This level quantifies water flows unbalance between the different elements of the SoS. It also quantifies flood risks and assesses the ability of the BHN complex to handle future floods for a mission period of 50 years.

Fig. 2. Multi-level modeling approach.

In this paper, only the 4th and the 5th levels are introduced and discussed. They correspond to the "Virtual Operator" and the "Orchestrator" respectively. Those levels are the building blocks of an algebraic representation of the states of our SoS with stochastic outcomes.

4. The virtual operator

The operator's task is to reroute the electrical energy flow and actively adapt to all new situations. Those events, whether planned or unplanned, are diverse (water management, outages, energy exports, ice cover, etc.). As a result, operators, who are highly skilled and trained, are constantly in an alert mode trying to solve, complex and evolving situations.

When it comes to mathematical modelling of real word situations, this poses a major challenge. A straightforward approach by modelling all combinatorial possibilities or operator free will, may be impractical. A balance between details and conservative assumption is key to a develop a reasonable model size and be able to compute an upper bound for risk. To downsize the problem, some reasonable assumptions are made: The operator is considered as a rational person, who favors switching sequence simplicity over efficiency. According to his role, he can minimize the impact of system failures in a short period of time (few minutes).

An inductive probabilistic method was developed to replicate operator decisions. The method navigates a stochastic graph from the "birth" of the system failure to the aggregate function of the generating capacity loss (Figure 3). In addition to its quantitative nature, such a technique highlights the resilience of the power system and its ability to minimize the loss of generating units during major events. This method was inspired by popular methods such as event tree analysis (ETA) (Marvin and Høyland, 2004).

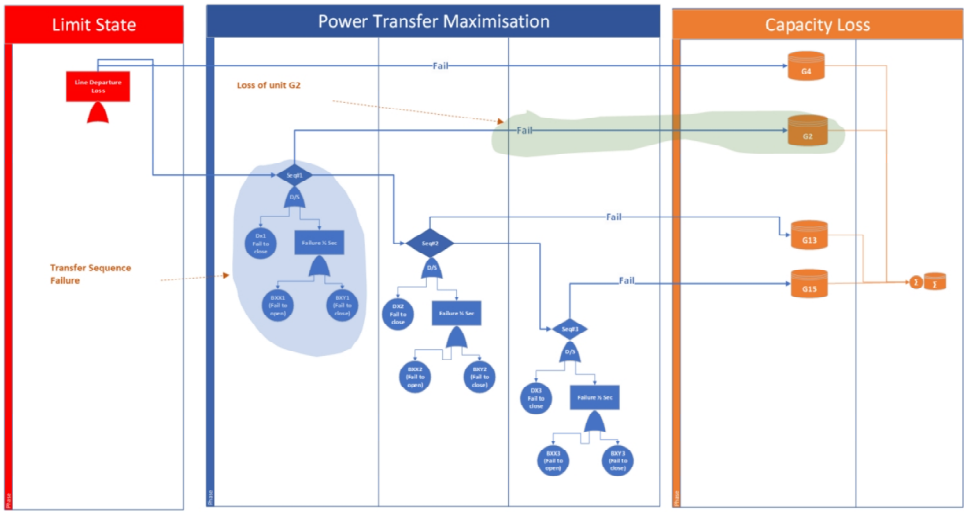

Fig. 3. Inductive method that measures the generating capacity loss based on operator switching decisions.

4.1. The inductive method

The innovative approach adapts to the context of BHN. It consists of a simulated acyclic event graph with the ability to aggregate results in multiple ways. Such approach gives more flexibility and expressiveness in modelling operator decisions compared to conventional Event Tree Analysis (ETA). In contrast to analytical approaches, the assessment of consequences is done through numerical approximation based on a Monte Carlo simulation. Three modelling phases are central to the method: (1) Limit State, (2) Power Transfer Maximization, and (3) Generating Capacity Loss.

First, the Limit State phase: The execution of the event graph begins with a system failure event consisting of the loss of one or multiple electrical subsystems (equivalent to an initiating event) that represents the degraded configuration of the power plant and a loss of a specific number of generating units. In practice, this Limit State places the power plant in a transitory post-disturbance degraded configuration for a few minutes before operator actions.

Second, the Power Transfer Maximization phase: To bring discharge capacity back to its maximum, or to its highest possible level, the operator must connect the tripped units through several switching sequences to the adjacent lines and eventually to different adjacent electrical systems. Switching sequences are carried out by the operator sequentially and chronologically and are validated using power flow simulations. The failure of the switching sequence leads to the definitive loss of the affected set of units.

Third, the Generating Capacity Loss phase: This part of the event graph, represents the counting process regarding unrecoverable unit losses. Information is given by counting (1) how many times a specific unit is lost, (2) and how many units are lost in total. A nonparametric and discrete probability distribution describing generating unit losses is derived from the simulation after the convergence is verified (Figure 4).

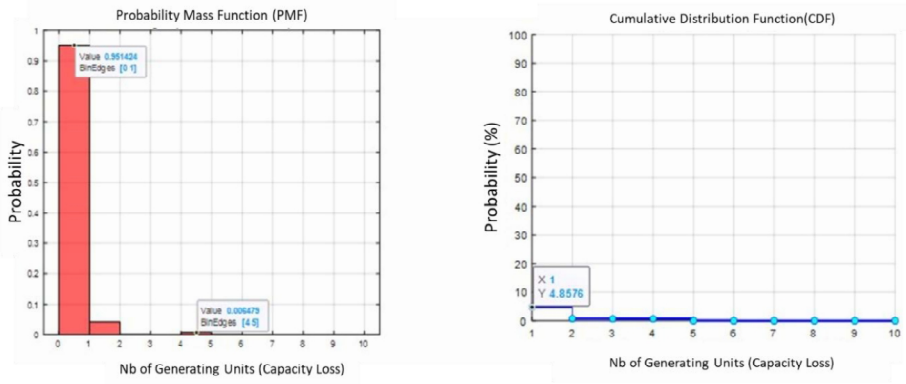

Fig. 4. Mass function and CDF of generating capacity loss.

4.2. The algorithm

In this section, we will briefly describe the algorithm behind the method. The term IE refers to the failure of a system or to an initiating event (Example: Power lines failure). It is usually due to a major event already explored using Fault Tree Analysis (FTA) in early steps of the project. We consider both failures of the system and the switching sequence as independent events. Each branch k of the graph represents the risk of losing one or a group of generating units as a result of a switching failure. Physical assets will be well maintained and are available for each critical mission. Each switching sequence is modelled as a series-system to show no tolerance for equipment failure in risky situations. Furthermore, reliability is the metric to use since physical assets are assumed to be nonrepairable during the flood period.

S_k denotes the switching sequence in the branch k of the graph. It refers to the set of all equipment operated during the sequence. For the branch k, the reliability of the sequence is evaluated by (1) or (2):

$$R_{S_k}(t) = \prod_{i\in S_k} R_i(t) = \prod_{i\in S_k}(1 - F_i(t)) \tag{1}$$

or

$$R_{S_k}(t) = \prod_{i\in S_k} R_i(t) = e^{-\int_0^t [\sum_{i\in S_k}^{|S_k|} \lambda_i(u)]du} \tag{2}$$

Therefore, the probability of a transfer sequence failure is given by (3).

$$F_{S_k}(t) = 1 - e^{-\int_0^t [\sum_{i\in S_k}^{|S_k|} \lambda_i(u)]du} \tag{3}$$

The failure probability of the transfer sequence S_k will be evaluated for the maximum duration of the flood D_{Flood} . For a very large number of simulations N we can successfully approximate this probability through simulations. Let's consider the indicator functions $I_{i,\left[t_{i,j}^* \le D_{Flood}\right]}$ that take their values in 0 or 1. $u_{i,j}^*$ are realizations of a uniform random variables over [0,1]. The failure probability of the transfer sequence will be given by (4).

$$p_{S_k} \approx \frac{\sum_{j=1}^{N}\left(\prod_{i\in S_k} I_i\left[F_i^{-1}\left(u_{i,j}^*\right)\le D_{Flood}\right]\right)}{N} \approx \frac{\sum_{j=1}^{N}\left(\prod_{i\in S_k} I_i\left[t_{i,j}^* \le D_{Flood}\right]\right)}{N} \tag{4}$$

When using the classical Inverse Transform Method, and for the special case of a constant failure rate we obtain the realizations of failure times by sampling u randomly over [0,1] as described in (5).

$$t_j^* = F_i^{-1}\left(u_j^*\right) = \frac{-1}{\lambda_i}\ln\left(1 - u_{i,j}^*\right) \tag{5}$$

With a Monte Carlo simulation, the failure probability of the transfer sequence S_k, for N very large is given by (6).

$$p_{S_k} \approx \frac{\sum_{j=1}^{N}\left(\prod_{i\in S_k} I_i\left[\frac{-1}{\lambda_i}\ln\left(1-u_{i,j}^*\right)\le D_{Flood}\right]\right)}{N} \tag{6}$$

In addition, by summing up the L graph branches we can estimate the number of unavailable generating units using a numerical approximation given by (7).

$$v_j = \sum_{k=1}^{L}\left[\prod_{i \in S_k} I_i\left[t_{j,k}^{*} \leq D_{Flood}\right]\right] \quad (7)$$

The different realizations v_j will follow a probabilistic and discrete distribution that captures the specific behaviour of the system.

When we use the indicator functions $I_{X_j=v_k}$ that takes its values in 0 or 1, and for N very large, the unavailable generating units will follow a discrete random variable that has a mass function described by (8). The cumulative distribution function is described by (9).

$$p(X = v_k|EI) \approx lim_{N\to\infty}\, p_N(X = v_k|EI) \approx \frac{1}{N}.\sum_{j=1}^{N} I(X_j = v_k) \quad (8)$$

$$F(X = v_k|EI) \approx lim_{N\to\infty}\, F_N(X = v_k|EI) \approx \frac{1}{N}.\sum_{j=1}^{N} I(X_j \leq v_k) \quad (9)$$

4.3. Simulation results

We have modelled dozens of event graphs to represent the most critical and unusual situations that the operator would have to tackle (busbar failures, double contingencies, power line failures, subnetwork common cause failures, etc.). 10^6 simulations were conducted to achieve convergence of results. Results are discrete probabilistic distributions and will be used as mitigation functions by the tool called the "Orchestrator" (Figure 5).

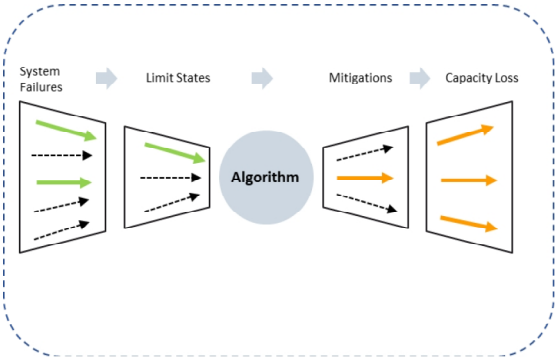

Fig. 5. Deductive-Inductive Method for the SoS.

5. The Orchestrator

In this section we introduce a novel approach for modelling system performance and safety. It proposes a new way to measure the performance at a system level for a transmission network. The algorithm that measures the Discharge Capacity is called the "Orchestrator". Its name describes its central role in modelling complex interactions between degraded states of the power plant and the appropriate decisions of the operator to mitigate consequences.

5.1. The method

In our approach, we are inspired by "Deductive-Inductive" approaches in reliability engineering. PRA studies are good practical examples used in the nuclear industry because of their effectiveness (Keller and Modarres, 2005). In fact, building a "Deductive-Inductive" logical approach for the Beauharnois SoS will be a powerful method for estimating the discharge capacity from logical combinations of system failures without losing details on their causes. This approach makes it possible to integrate the operator logic in its complexity, which is key to modelling the resilient behavior of the SoS.

5.2. The algorithm

We use Boolean Algebra properties to derive the state function of the system thanks to Shannon Expansion in minimal terms (Shannon, 1949). So, for N Boolean variables, and f a Pseudo-Boolean function, we have the (10).

$$f(X_1, X_2, X_3, \dots, X_n) = [X_1 . f(1, X_2, X_3, \dots, X_n)] + [\bar{X}_1 . f(0, X_2, X_3, \dots, X_n)] \quad (10)$$

The equation can be expanded for the variable X_2, and iteratively for all variables X_i as in (11).

$$\begin{aligned} & f(X_1, X_2, X_3, \dots, X_n) \\ & = [X_1 . X_2 . f(1,1, X_3, \dots, X_n)] + [X_1 . \bar{X}_2 . f(1,0, X_3, \dots, X_n)] + [\bar{X}_1 . X_2 . f(0,1, X_3, \dots, X_n)] \\ & + [\bar{X}_1 . \bar{X}_2 . f(0,0, X_3, \dots, X_n)] + [\bar{X}_1 . X_2 . f(0,1, X_3, \dots, X_n)] + [\bar{X}_1 . \bar{X}_2 . f(0,0, X_3, \dots, X_n)] \end{aligned} \quad (11)$$

Hence, the use of this fundamental property is very interesting since it ensures two essential aspects of our modelling. First, it encodes multiple states of the system using a combination of variables expressed in simple Boolean terms (Working state:0, Failed state:1). Second, it enables only one term of the equation, at a time, to be activated during the simulation. This activated term will execute the mitigation function. Subsequently, all Boolean variables are replaced with random variables to deal with the probabilistic nature of system states and mitigation.

For instance, let's model the loss of generating units for a generic power system composed of five subsystems: two power generating subsystems, two bus bars, and one power line. The mitigation function is also a random variable. It measures the number of unavailable generating units during the flood mission because of busbar or power line failures. This generic case corresponds to an 8-term equation (2^3 encoded states). Equation (12) combines uncertainty about system states and mitigation (Figure 6).

$$\begin{aligned} & M(B_i, B_j, L_k) = [B_i . B_j . L_k . M(1,1,1)] + [B_i . B_j . \bar{L}_k . M(1,1,0)] + [B_i . \bar{B}_j . L_k . M(1,0,1)] + [\bar{B}_i . B_j . L_k . M(0,1,1)] \\ & + [B_i . \bar{B}_j . \bar{L}_k . M(1,0,0)] + [\bar{B}_i . \bar{B}_j . L_k . M(0,0,1)] + [\bar{B}_i . B_j . \bar{L}_k . M(0,1,0)] + [\bar{B}_i . \bar{B}_j . \bar{L}_k . M(0,0,0)] \end{aligned} \quad (12)$$

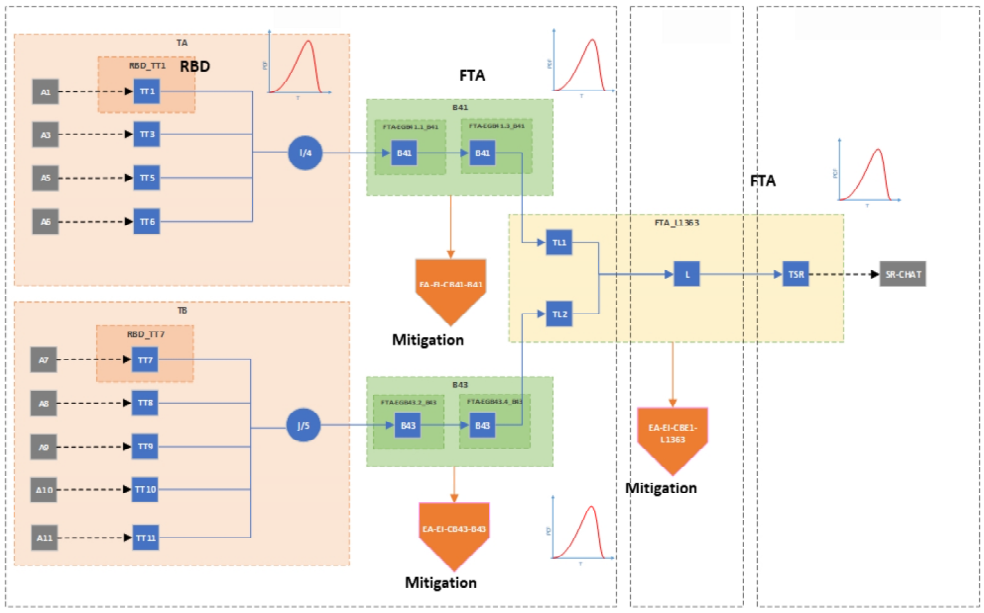

Fig. 6. Generic Power System Layout (Functional Layout).

To give an intuition about the model, we propose a graphical representation, inspired by Binary Decision Diagrams (Akers, 1978); (Figure 7).

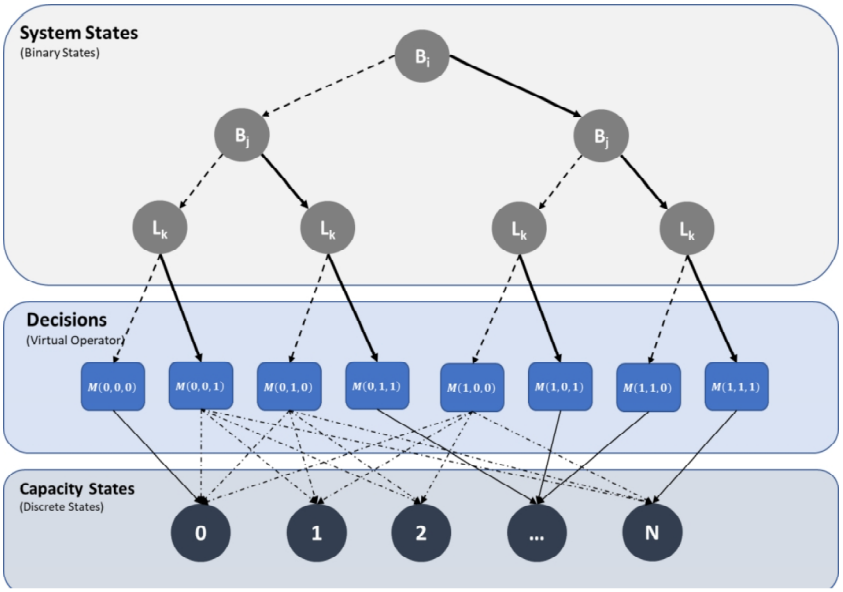

Fig. 7. Graphical Representation of Probabilistic System State Function.

The final model for the entire generic power system will include two additional power-generating subsystems where mitigation is not possible. This model is described by (13).

$$N_{PS} \cong N_{T_A} + N_{T_B} + \left[B_i.B_j.L_k.M(1,1,1)\right] + \left[B_i.B_j.\bar{L}_k.M(1,1,0)\right] + \left[B_i.\bar{B}_j.L_k.M(1,0,1)\right] + \left[\bar{B}_i.B_j.L_k.M(0,1,1)\right] + \left[B_i.\bar{B}_j.\bar{L}_k.M(1,0,0)\right] + \left[\bar{B}_i.\bar{B}_j.L_k.M(0,0,1)\right] + \left[\bar{B}_i.B_j.\bar{L}_k.M(0,1,0)\right] + \left[\bar{B}_i.\bar{B}_j.\bar{L}_k.M(0,0,0)\right] \quad (13)$$

For the flood mission, and after simplification, N_{T_A}, N_{T_B} follow binomial distributions and B_i, B_j, L_k follow Bernoulli distributions. All parameters of those distributions are calculated using previous reliability models including Fault Tree analysis and Reliability Block Diagrams. The mitigation function $M(B_i, B_j, L_k)$ is evaluated using Operator Event graphs as seen in the virtual operator section.

The model of the Beauharnois SoS is a large model. It includes spills caused by the failures of 12 different power lines departures (LD) and 8 multi-contingency failures of 4 adjacent subnetworks (SN). The number of unavailable generating units is described by (14).

$$N_{BHN} = \sum_{LD \in \{All\ Power\ Line\ Departures\}} N_{PS} + \sum_{SN \in \{All\ subnetworks\}} N_{SN} \quad (14)$$

5.3. Simulation results

The simulation framework was coded in the R language. Figure 8 shows actual Orchestrator simulation results, as well as the different data processing steps required for the exercise.

The algorithm output gives, for different risk levels (from 10^{-1}/year to 10^{-6}/year), the expected maximum number of unavailable generating units. Therefore, the discharge capacity, assured by the transmission network, is determined easily by using the remaining available capacity. For the decision maker, this sets an easy ground discussing acceptable risk levels without dealing with probability and abstract concepts.

Interesting and surprising results were derived especially regarding the system reliability and resilience. In fact, simulation helped uncover blind spots like operator role and network topology impact on the discharge capacity. For instance, Figure 9, highlights exceptional system resilience for high-impact low-frequency events when Network topology is improved.

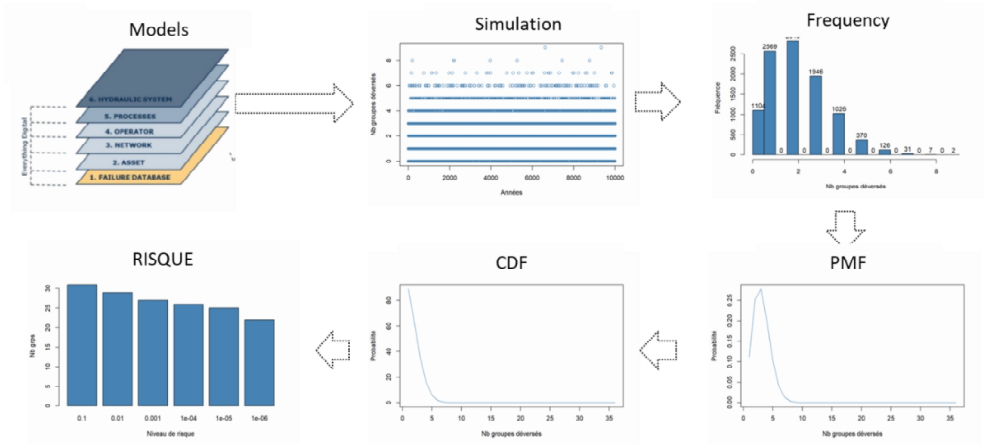

Fig. 8. Simulation Process.

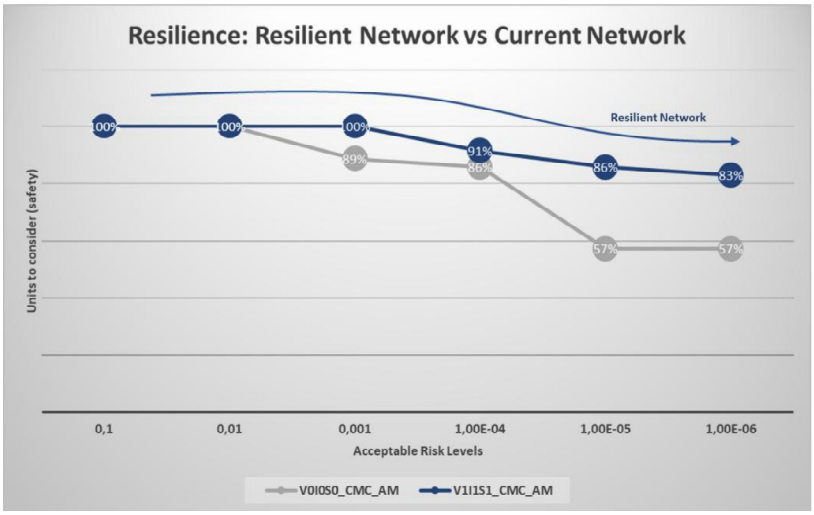

Fig. 9. Available generating capacity by risk level (Resilient Network vs. Current Network).

6. Conclusion

Large and complex systems such as “Beauharnois-Les Cèdres” are becoming ubiquitous and they present a new challenge for engineers and professionals in the reliability field (Komljenovic, 2019). In fact, this SoS imposes the use of reliability techniques and power flow simulations simultaneously to be able to give a realistic and probabilistic view of it. Furthermore, many of the discoveries about its behavior, like resilience (Bellè, 2022), are counterintuitive and difficult to model or capture using conventional reliability methods.

To achieve the objectives of the project, novels approach, and several scientific methods have been developed to tackle the complexity. They are presented as follows:

- a new electrical methodology was able to pave the way for reliability analysis by simplifying the electrical model and focusing only on critical and relevant system states without loss of accuracy;
- a Multi-Level modelling framework for reliability analysis was developed to integrate all models at different abstraction levels;
- a new inductive and quantitative reliability method was proposed and was able to capture the operator rational behavior by modelling post-contingency mitigation using event analysis;

- a simulation framework called “Orchestrator” was developed to act as a “Rule Engine” between simulated system states and operator actions. This level was able to take in charge all models outputs of all subsequent levels and recreate the dynamics between failed states and system reconfiguration. Everything is effectively captured using a single and unified algebraic model for the SoS.

In the future, more aspects of electrical network resilience have to be explored. To that end, those methods can be improved by adding the power of graph theory in modelling electrical networks (Dersin, 2022) and the agility of agent-based modelling when dealing with system adaptability.

References

Akers, 1978. Binary Decision Diagrams, in IEEE Transactions on Computers C-27(6), 509-516.

Bellè, A. 2022. Resilience and coupling of interdependent critical infrastructures: models, optimization, and operations. Diss. Université Paris Saclay.

Dahmann, J.S. 2015. Systems of systems characterization and types. Systems of Systems Engineering for NATO Defence Applications, 1-14.

Dersin, P. 2022. Resilience and Capacity in Networks - A comparative Investigation of Rail Transport Networks and Electric Power Grids. 60th ESReDA Seminar, Grenoble.

Keller, W., Modarres, M. 2005. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry. Reliability Engineering and System Safety 89. 271–285.

Komljenovic, D., Abdulnour, G., Boudreau, J. 2019. Risk-informed decision-making in asset management as a complex adaptive system of systems. International Journal of Strategic Engineering Asset Management. 198-238.

Komljenovic, D., Messaoudi, D., Larivière, P., Caron, S., Chahine, R. 2019. Risk-Informed Decision-Making in Asset Management of Electrical Utilities. CIGRE Canada Conference, Montreal.

Marvin, R., A. Høyland, 2004. System Reliability Theory Models, Statistical Methods, and Applications. Wiley.

Shannon, C. 1949. The Synthesis of Two-Terminal Switching Circuits, Bell System Technical Journal, 59-98.