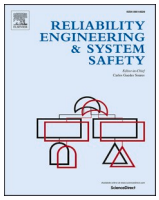
Reliability Engineering and System Safety 238 (2023) 109450

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress



A human operator model for simulation-based resilience assessment of power grid restoration operations

Felix Kottmann [a,*], Miltos Kyriakidis [b], Giovanni Sansavini [c,*], Vinh Dang [b]

[a] Future Resilient Systems, Singapore-ETH Centre, Singapore
[b] Laboratory for Energy Systems Analysis, Paul Scherrer Institute, Switzerland
[c] Reliability and Risk Engineering, ETH Zürich, Switzerland

A B S T R A C T

Human operations play a vital role for the resilience of power grids. While past research concentrated on performance in cascading failures, this work proposes a system model that focuses on assessing the impact of the performance of operators in grid operations and restorations. The operator model developed for this purpose addresses human performance and variability by accounting for stochastic durations, potential errors and alternative responses, and the probabilities of these outcomes. Discrete event simulation is the assessment framework, with the model implemented in MATLAB Simulink in conjunction with a dynamic power system model. A re-energization cell provided by a Swiss generation system operator is used for a case study demonstration of the simulation model, which produces distributions of the total restoration duration and restoration success rates while identifying the parts of restoration plans that could be modified to enhance restoration performance. The overall outcomes of the case study suggest that the human element can be treated practically in grid simulations in order to produce findings that will increase grid resilience.

1. Introduction

Recent years saw increased stress on electric power grids, exemplified by the Texas black-out and two grid splits in the European ENTSO-E grid in 2021 [1,2], due to increasing risks by severe weather [3], market [4] or volatility of renewables [5]. To mitigate those risks, the power grid's resilience has been identified as crucial [6], addressing the ability to withstand disruptions and absorb and recover from them. The U.S. National Academy of Sciences identifies planning, preparation, reaction to disruptive events, endurance and damage assessment, restoration, and recovery as essential to a grid's resilience [7].

Fast and reliable restoration is a significant contributor to power system resilience after major disruptions such as blackouts [8]. Depending on the blackout extent, the restoration is either top-down, i.e. supported by other energized parts of the grid, or bottom-up, i.e. by forming electrically stable islands around black-start capable generators that are eventually connected to the grid.

Restoration performance has been either assessed individually or as part of an infrastructure resilience assessment, also covering the absorption capacity of the system after a shock. Particularly, restoration has been assessed in conjunction to repair after physical damage. Its performance has been either assessed by models of the repair and restoration co-optimization [9,10], or by discrete simulation, subject to logistical impacts [11]. Further, the duration distributions of restoration plans have been assessed *via* Petri nets [12] and *via* the critical path method [13]. Other work has assessed and described restoration performance *via* statistical analysis of past incidents [14,15]. While Duffey [14] describes the progress of the restoration of normalized past restoration times, Čepin [15] presents the anticipated completion time distribution as exceedance probabilities within a probabilistic safety assessment framework.

Resilience assessment frameworks that include restoration build the restoration sequences either around heuristics or optimization algorithms, as the extent and location of blackouts might be unpredictable, e.g. due to cascading effects. However, most approaches, e.g. Beyza et al. [16], generate such restoration sequences without considering operational or dynamic limitations. Those technical constraints have been covered in research on restoration and focused predominantly on planning and optimization with technical considerations, such as black start, transient stability, inrush currents, or restoration sequence optimization [17,18]. As of today, restoration remains a highly manual process, reliant on human operators [19,20] and limited by corporate boundaries [21,22]. Also, discussions led by the industry on the potential of automation in the restoration process, such as in recent work by Bosch et al. [23], acknowledge the sustained relevance of human operators in the process.

* Corresponding authors.
E-mail addresses: felix.kottmann@sec.ethz.ch (F. Kottmann), sansavig@ethz.ch (G. Sansavini).

https://doi.org/10.1016/j.ress.2023.109450
Received 14 November 2022; Received in revised form 20 May 2023; Accepted 11 June 2023
Available online 16 June 2023

Explicitly, human performance in restoration has only been studied subject to stochastic task durations [12,13]. Further, human factors were considered only implicitly, if at all. For instance, Duffey [14] fitted a learning hypothesis model to normalized restoration performance data of several events to explain the performance increase over the years.

Furthermore, human failure and the risk of deviations or component damage, caused by human errors, during the restoration process have not been evaluated. Indeed, during restoration, operational security principles, such as the N-1 principle in electric power systems, may not be satisfied, which increases the risk of system re-collapse. Edström and Söder [24] investigated this risk during restoration subject to stochastic component failure, and by the loss of backup power [25]. Such a re-collapse results in a deviation from the restoration plan and, thus, in delays or even component damage. Therefore, restoration planning must also account for human performance *via* the modeling of dedicated tasks, and the related human failure, situation assessment, and decision-making. To better understand the general role of human operations and its positioning in research, Guttromson et al. [26] investigated the role of human factors and situation assessment in the operations of power grids by analyzing the Northeast blackout of 2003. The authors acknowledge that methods can be borrowed from the vast field of human factors research considering the nuclear power domain. However, differences are identified as a power grid is an open system with various entities observing different states and controlling different components. Human factors have been studied in control room environments, particularly in the nuclear power generation sector.

Human reliability assessment (HRA) frameworks can be divided into first-generation methods, such as THERP, HEART, and SPAR-H and second-generation methods, such as ATHEANA and CREAM. While first-generation methods rely on atomic task decomposition, second-generation methods also describe and include the context in order to derive human error probabilities [27]. As of today, methods of both generations remain in use. New developments enhance those methods, e.g. by expert judgment or coupling with the system state, such as in Zhao and Smidts [28]. Human factors in power grid operations have been mostly studied in the context of cascades. Li and Blanc [29,30] describe the operator tasks during cascading failures using work domain analysis to account for the human contribution to performance and risk. Their study suggests various methods, such as cognitive models or HRA methods. Simulation-based results are shown by Shuvro et al. [31,32] and Wang et al. [33], who use the SPAR-H HRA methodology in a dynamic setting to determine whether an operator successfully stops the progression of cascading failures. Zhou et al. [34] measure the physical stress of dispatchers to determine SPAR-H performance shaping factors (PSFs) and predict human error probability. However, those models do not focus on the execution of plans or of complex tasks and do not implement the necessary level of detail for capturing the contribution of human performance on complex tasks [29,30]. Hao and Qun [35] present a model for emergency dispatch in the presence of hidden faults. Their study uses the Human Cognition Reliability Model, which application, however, is limited to determining whether a control room crew answers correctly a safety-critical event in time [36]. Further, a steady-state power flow model is employed which is not capable of simulating the dynamic effects relevant during the restoration process. Nan and Sansavini [8] present an assessment framework that allows for assessing infrastructure systems for a various set of resilience metrics. Their model contains a steady-state DC power flow and a human operator model, reacting to alarms, using the CREAM methodology. In a similar approach, Magoua et al. [37] present a high-level architecture for the simulation of interdependent critical infrastructure systems with each infrastructure system capable to be encapsulated with its own model. Their presented case study considers an operator in response-driven operations where a CREAM human factors model is used. In a case study, an interdependent power- and water system is simulated under a failure scenario that requires the handling of false overloading alarms to avoid component tripping. Results consider the number of failed tasks and the dynamic evolution of HEP.

However, the aforementioned studies of human factors in power grid operations focus on either single tasks or responses within cascades, a context that differs significantly from the plan-driven operations in restoration [38]. Hence, more comprehensive frameworks are needed to simulate the execution of plans and allow to derive performance and risk metrics. Most frameworks that employ HRA methods aim to derive a (dynamic) probabilistic safety assessment, identifying undesirable trajectories, their outcome, and their probability [39]. To derive all relevant trajectories and their probabilities, approaches either rely on an explicit representation, such as *via* event trees or event-sequence diagrams, or implicit methods, such as Monte Carlo simulation. Recent work by Bolton et al. [40] has explored formal methods to identify all undesirable states. However, such an approach requires a full description of the system in temporal logic. Such a description might be difficult to derive due to extensive modeling effort and traditional PSA might not be sufficient as details of accident scenarios are lost due to the grouping. Instead, Cho et al. [39] suggest an approach of exhaustive simulation to determine a wide range of scenarios individually in a PSA. A similar approach was chosen by Shin et al. [41], who follow the System-Theoretic Accident Model and Processes. Control actions performed by human operators are assessed in a combined model of a human operator, information and communication system, actuators, and the controlled process. Their approach defines boundaries, models the control system structure, identifies unsafe control actions, and identifies loss scenarios. However, in restoration, the major challenges do not necessarily root in the control structure but rather in the human operations and dynamic system responses, such as frequency transients. Hu et al. [42] further narrow down the simulation effort by an engineering-knowledge-guided simulation approach of high-level plans within the information, decision, and action in crew context methodology. This methodology achieves a dynamic PSA to explore undesirable outcomes, the branches that lead to them, and the probability of those end states.

Since restoration operations are mostly trained in simulators and live exercises, taking place every 6 months to 2 years [43,44], adequate data to support the application of statistical approaches is not available at this time. Hence, this work addresses the assessment of restoration operations through discrete event simulation. This modeling approach allows the estimation of restoration durations (in terms of distributions), the identification of potential error scenarios, and the examination of the consequences and recovery options for these scenarios. Such results support the revision and enhancement of restoration plans and may provide scenarios and priorities for power grid operator training.

Motivated by this gap, this work aims to capture the critical drivers of restoration performance and variability, identified as human operator related. Our contribution is a human operator model, capable of treating stochastic task durations and the error outcomes of tasks, decision-making, situation assessment, and an alternative mode of operation, caused by time pressure. To quantify resilience, calculated metrics for the recovery process include task durations, composite human failure probability, and decisions on responses to encountered deviations.

This work has been carried out in collaboration with the Swiss national Transmission System Operator (TSO) Swissgrid and Kraftwerke Oberhasli (KWO), a regional generation system operator (GenCo). While Swissgrid is responsible for the country's restoration plan, KWO provides one of the restoration cells that form its root.

This paper is presented in the following sections: Section 2 gives an overview of the operations of power grids, leading actors, and their conduct. Section 3 describes the conceptual human operator-grid model and its implementation. Section 4 presents the case study on the KWO restoration cell re-energization. Section 5 shows the results and discussion, and the paper concludes with Section 6.

Table 1
Tasks of TSOs, DSOs, and GenCos (adapted and modified from Ref. [51]).

Role	Tasks
TSO	- Switching of equipment, such as transmission lines and transformers - Change of setup or parameter values, e.g., transformer taps - Re-dispatch of generation and load - Switching of loads
DSO	- Switching of equipment, such as transmission lines and transformers - Change of setup or parameter values, e.g., transformer taps - Switching of loads - Power plant operator actions if DSO operates power plants
Gen-Cos	- (Black-) Start or stop of generator / pump - Synchronization of generator - switching of generator / pump - Change of generator / pump specific parameters, e.g., control mode

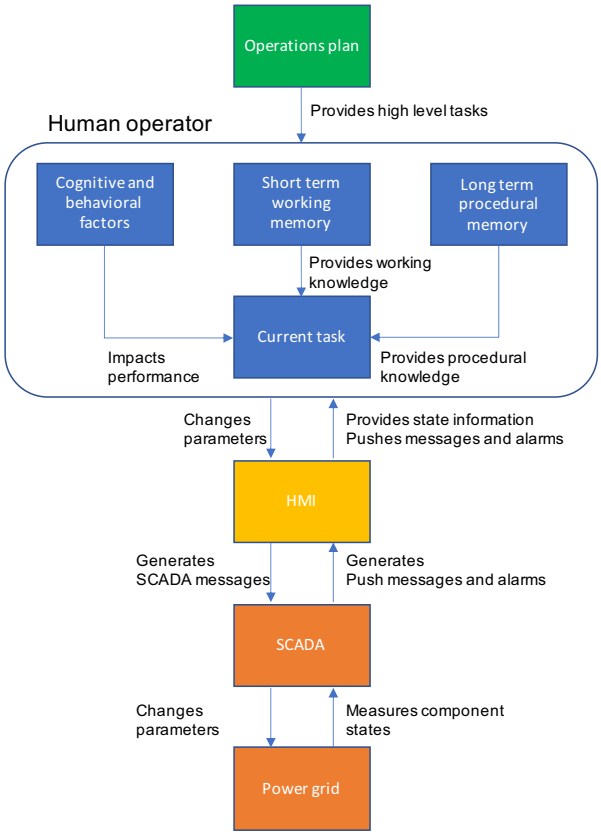


Fig. 1. Conceptual model of the human operator and its interaction with the operations plan and power SCADA system. Green: Plan, blue: Human operator, yellow: Interface (HMI), Orange: SCADA and power grid.

2. Operations in power systems

This section presents the overview of power system operations, including the relevant actors, roles and responsibilities, and interaction with human-machine interfaces (HMIs). An overview of the different operational states and the most common task types is presented to highlight the circumstances of the restoration process. All descriptions are derived from the ENTSO-E guidelines [38,45–49], and interactions with Swissgrid and its member organizations.

2.1. Organization of grid operations: responsibilities of TSOs and DSOs

In most European countries, the power grid is operated as one connected synchronous area. International associations, such as the ENTSO-E, are responsible for formulating and overseeing policies and guidelines for a synchronous area but are not directly involved in operations. Three entities are mainly engaged in operations, TSOs, DSOs, and GenCos. TSOs supervise the operations of higher voltage levels of the transmission grid and ensure grid stability in terms of frequency, voltage, and transmission line loading levels [46]. DSOs are responsible for controlling local distribution grids and parts of the lower voltage levels of a national grid [46]. Finally, GenCos are responsible for feeding in power [45,49].

2.2. The role of plans, procedures, and responses

Control room staff of TSOs, DSOs, or GenCos follow a written plan consisting of an ordered sequence of tasks for their daily operations. Procedures are developed by each organization to establish an agreed reliable way to conduct all tasks [50]. The scope of operations varies depending on the grid's operational state, which is classified as: normal mode, alert (N-1) mode, emergency mode, partial or full blackout, and restoration [38]. Along this sequence, manual operator tasks are increasingly required to bring the power grid to its normal state [46,47].

After a blackout, the responsible TSO initiates the restoration process. DSOs and GenCos may also be involved in the restoration according to the TSO's restoration plan. Such a restoration plan is formulated beforehand or amended depending on the situation [38], and defines the steps of black-start, re-energization, re-synchronization, and load pick up. Depending on the black-out size and grid conditions, a bottom-up or top-down restoration approach is chosen [47]. The former starts at the black-start and forms islands, while the latter begins directly with the re-energization of the grid utilizing its energized parts. According to the requirements of the TSO restoration plan, the DSOs and GenCos involved in the restoration formulate their plans to execute their assigned tasks. Deviations to a restoration plan might occur due to failures or unavailability of equipment. In such cases, operators initiate appropriate responses, which are contingency measures, aiming to re-create a state allowing the resumption of the restoration plan. Those responses comprise a clustered sequence of tasks and are defined by a procedure in which operators have been trained multiple times per year [46].

2.3. Operator tasks

Table 1 summarizes the most common task categories performed by the TSOs, DSOs, and GenCos. Tasks are included in the operating plans or are part of the procedures, as specified in Section 2.2. Each task is modelled using the task template in Sections 3.2.1 and 3.3.2.

2.4. HMI interfaces and overhead displays

TSOs, DSOs, and GenCos perform their duties in control rooms equipped with overhead displays (OHDs) and computer workstations that build the human-machine interface (HMI), enabling the interaction with the supervisory control and data acquisition (SCADA) system. OHDs provide schematic overviews of the system, color code the operational state of its components, and push audiovisual alarms to the operators [52–54].

Operators interact with the power system through dedicated software as part of the HMI. The high-level states of the system's components, such as the energization status of bus bars, are displayed on a main display, comparable to a home screen. In contrast, the more detailed parameters of the system, such as set voltages of generators, are available *via* sub-menus and different control screens. Any changes in the parameters are implemented *via* clicking on visualized elements, check-boxes, or (radio) buttons, as well as entering numerical values, or modifying numerical values (increasing or decreasing) *via* arrow buttons.

3. The human performance simulation model

3.1. Scope

The operators' performance is assessed in terms of time and human failures by simulating the operations of an island grid serving as restoration cell within one corporate organization. The human operator model executes a given plan and reacts to possible deviations in the evolution of the grid state. Thus, it covers variability in task execution time, probabilistic determination of errors, situation assessment of the grid state and decision-making reacting to a deviating grid evolution. Similar to Ref. [55], human failures include mistakes, expressed as planning and situation assessment errors [26], slip errors in task executions, and lapses in memorized procedures [55]. Violations are not within the scope of this work. Responses to deviations in the grid evolution aim to return to the initial plan. Given the full system observability and controllability *via* SCADA, no oral communication is modeled in this framework. For simplification, the crew is modeled as one operator. Finally, we postulate an alternative mode of operations, when operators under system- and time-critical conditions might accelerate the execution time while facing higher risk of slip errors.

3.2. Conceptual model

Fig. 1 presents the conceptual human operator model and its interaction with the operations plan and power grid *via* the HMI and SCADA system.

The power grid represents an isolated grid consisting of generators, pump storage, transmission lines, bus bars, transformers, switches and breakers. Due to the design following the separation of concerns principle [56], the power grid might be extended with other power system components, such as HVDC transmission lines.

The human operator's memory consists of the working memory (short-term) and long-term procedural memory. The working memory keeps track of the operational parameters and abstractions, such as system frequency. The long-term memory comprises task and procedural knowledge, such as responses to deviations. Cognitive and behavioral factors are task and operator-dependent and impact the operator's ability to perform tasks, assess a situation, and decide on responses. These comprise particularly the operator's time performance and probability of errors.

3.2.1. Model of simulated process, plans, responses, and tasks

The simulated process is determined by the scenario input, which provides an operations plan, the operator's responses from previous training, and the parameters for each task. The plan defines an ordered sequence of tasks. Procedures, such as the re-energization procedure, describe the execution of the plan and its tasks. Tasks are set patterns of actions [57] and may include sub-tasks. Actions can either be cognitive (mental) activities, such as reading a parameter from the HMI, or execution activities, such as closing a breaker.

To formalize the task types shown in Table 1, the conceptual model introduces task templates, which are part of the long-term procedural memory and describe the procedures of tasks and sub-tasks. A task template specifies for each task type the necessary parameters to be monitored or manipulated, error outcomes, and describes the temporal execution of its actions. Tasks share similarities but differ in the number, type, and temporal sequence of actions or might also involve mental subtasks such as the computation of parameters. Hence, each task is represented by a dedicated task template.

3.2.2. Situation assessment, decision making, and responses

Alarms inform the operator in the case of equipment failure or violations of operational ranges. Operators assess the situation by identifying the alarm cause and current topology. Then, they decide on a response. A response is described by a procedure and defines a starting condition, i.e., a topology state (indicating the connection status of components), a resumption step in the plan, and all necessary tasks to achieve the topology at the resumption step.

ENTSO-E guidelines on operation and restoration suggest that operators avoid operating a system within a state and topology they are not familiar with Refs. [46,47]. When a topology does not match any response's starting condition, the operator aims to achieve the closest possible starting condition by always reducing the topology. This reduction is achieved by disconnecting pumps, generators, transmission lines and transformers in this order, while ensuring frequency stability in between the switching tasks.

3.2.3. Model of human performance

Human performance covers the outcome of tasks as specified in task templates and might be success or error outcome. Situation assessment errors cover the incorrect or incomplete assessment of the system state [26]. Planning errors address erroneous judgment of impacts of actions on the components and system state subsequent to a response. Slips are actions wrongly executed, while lapses are errors related to the memory of parameters and tasks part of responses [55]. Task-based errors are defined for every task type in the task templates and specify the realization of the error, e.g. the over-correction of the frequency transient by the operator after a pump connection or generator synchronization. Scenario-based errors are defined by the scenario narrative and occur only when the unique task or situation arises. This might be an incorrect situation assessment after a given component trip (disconnection of a component) that causes a different response than usual or a different outcome of a task, such as the change of a generator control mode within the synchronization preparation.

The outcome of a task might be implemented deterministically or determined stochastically, if more than one outcome has been specified. To assign probabilities on potential error outcomes, a Human Reliability Analysis (HRA) method, such as SPAR-H [58] might be leveraged.

3.2.4. Model of time performance

The durations of tasks comprise the operator's perception, cognition, and action by interacting with the HMI [59], and technical overhead time, such as the starting of generators. Task durations are described by probability distributions. To account for the dynamics of time performance, such as the characterization of a slow or fast crew, our model supports the dependence of durations among subsequent as further described in Section 3.3.3.

3.2.5. Alternative mode of operations

Throughout the operations under critical conditions, operators might undergo a change of state of mind, resulting in a different mode of operations compared to the initial – nominal – mode of operations. Contrary to the assumption of most HRA techniques, our work proposes a new contribution to treating slip errors. Instead of implicitly treating slip errors and their recovery within the modeled time [58], our approach always treats those explicitly since slip errors – if executed – have a direct impact on the system state. This is achieved by (1) allowing less time for the task execution, i.e. shorter task duration, and (2) increasing the probability of slip errors with their outcome applied directly to the system, i.e. different HEP conditions. If an erroneous outcome causes a deviation to the plan, the recovery is to be simulated explicitly under the alternative mode of operations which is facilitated in the conceptual model. A transition to the alternative mode might happen at defined points which are referred as "pivotal points" in the remainder of this work. The features contributing to the transition into the postulated alternative mode of operations are further classified as operator-dependent and external situation-attributed features.

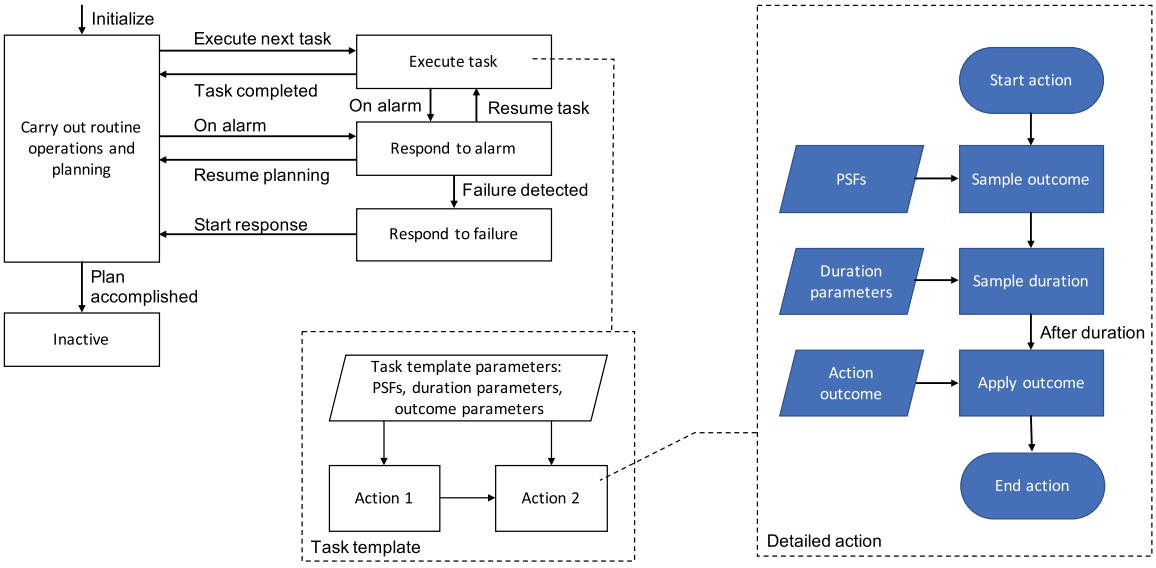


Fig. 2. Human operator state machine, a nested task template and its detailed implementation as a flowchart.

3.3. Implementation

3.3.1. Simulation framework, power grid, and SCADA

During restoration, a key driver to component tripping are particularly frequency transients and inrush currents. To account for transients in the simulation, a dynamic power grid continuous time power system model is required, while operator actions require a discrete event model. The MATLAB Simulink [60] platform was chosen to implement the joint hybrid model, allowing for Monte Carlo discrete event simulation of the restoration process. Stateflow [61] and Simevents [62] libraries were utilized to implement the human operator and SCADA communication layers. The dynamic power grid model was implemented with the Simscape Electrical [63] library, which provides detailed models of all components and allows for dynamic simulation. The high-level structure is shown in Fig. 11 in Appendix 1. Based on actions to be executed, SCADA messages are generated by the human operator model and routed to the respective components. The components' SCADA interfaces translate received information into specified parameters, such as breaker status, impacting the power grids' state. Further, continuous measurements and discrete push-messages are generated at all component models and forwarded to the human operator model.

3.3.2. Human operator modeling

The main activities of a human operator during power grid restoration are the execution of tasks, routine operations and planning, and the response to alarms or their causes. Hence, the human operator's mental state and activity are modeled as a state machine, which has been applied successfully before in the context of human-machine interaction [64,65] illustrated in Fig. 2. The main states are: "carry out routine operations and planning", "execute task", which can be part of a plan or response, "respond to system failures", "respond to alarms", and "inactive" (simulation terminated). As exemplarily shown in Fig. 2, task templates are implemented as nested state machines within the "execute task" state. The situation assessment is nested within the "respond to alarms" state. The decision on responses and the creation of their initial topology is nested within the "respond to failure" state. Responses are implemented along the operations plan in the "carrying out routine operations and planning" state. Transitions within task templates and situation assessment are timed to implement task durations sampled with the tasks' duration parameters as indicated in the detailed action flowchart in Fig. 2.

The functions called by the state machine have direct access to the OHD and HMI values and implement manipulations to the grid as SCADA messages. Working memory variables are accessible to all task templates to store observations of system frequency, bus bar voltages, and component states. Alarms are implemented as push messages to the operator, triggering a transition to the "respond to alarms" state.

In the execution of a plan, the next task struct is read from the plan in the state "Carry out routine operations and planning" into the working memory. Subsequently, the state machine transits to the state "execute task," which calls the task template specified by the task type and arguments in the task struct. Upon completion, the state machine transits back to the state. All modelled tasks are shown as flowcharts in Appendix 6.

In the case of an alarm, the state machine transits to the state "respond to alarms" where the alarm message data is evaluated. If tripping has occurred, the state machine transits to the state "respond to failure". In that state, the current topology Top_t is assessed from the component status values available from the OHD function. Subsequently, the decision on the response is determined by selecting the response i with the closest starting topology Top_i which can be achieved by only opening breakers. The mathematical rule implemented is

$$i = \underset{i}{\operatorname{argmin}}\left\{ ||Top_t - Top_i||_2 \mid Top_t - Top_i \geq 0 \right\} \tag{1}$$

where, Top_t describes the binary vector of the current switching status of all components and Top_i the switching status of response i's starting topology. For the subsequent opening of breakers, hard-coded priorities of breakers ensure the removal of pumps, generators, transmission lines and then transformers in this sequence to limit transients impacting the frequency stability while creating initial conditions to a response. Further, to maintain frequency stability, each response defines a target frequency and a reference bus, where the frequency is to be measured. While in the response state, opening of breakers and frequency correction are executed iteratively until the starting topology and frequency of the decided response are met. Subsequently, the state "carry out routine operations and planning" is activated and the response tasks are executed. When all response tasks are executed, the operator continues with the plan at the resumption step defied by the response. A flowchart-representation of this procedure is shown in Appendix 6.

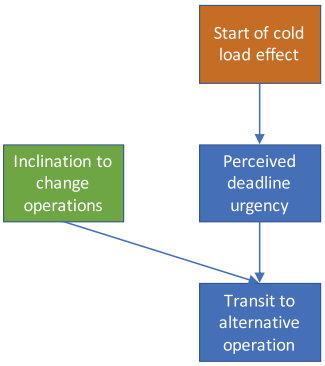


Fig. 3. Bayesian Believe Network to determine the transit to the alternative mode of operations.

3.3.3. Determination of error probabilities

Human failure events are explicitly defined as error outcomes in the task templates, while scenario errors might differ from the specific task-based error and require a distinctive, hard coded task template. To treat human failure events probabilistically, our approach employs a HRA [27] method to derive a human error probability (HEP), accounting for the impact of various PSFs, such as training or the adequacy the HMI.

HRA methods are commonly grouped into first and second-generation methods [27]. First-generation methods, such as THERP and SPAR-H, tend to atomize tasks and treat PSFs independently. Second-generation methods, such as CREAM and ATHEANA further consider the cognitive aspects of tasks in the process of decomposition. While the conceptual model allows for all methods that compute a HEP based on a range of specified PSFs, this work utilizes the SPAR-H methodology [58]. It is chosen as it provides a systematic methodology to derive a HEP based on the task type – action or diagnosis – and PSFs for control room settings. Further, reference values are available for switching tasks from interviews [34,66] and its application has been demonstrated in power-grid-related studies [32,34,66].

SPAR-H describes the relationship and values of eight PSF multipliers. Those are available time, stress/stressors, complexity, experience/training, procedures, ergonomics / HMI, fitness for duty, and work processes. Our approach additionally classifies the stress/stressors and fitness for duty PSFs as operator-specific PSFs and the remaining six PSFs as task-specific. Operator-specific PSFs are assigned equal for all tasks based on the operator, while task specific PSFs are assigned for every task specifically.

3.3.4. Task duration distributions

Previous work has suggested the use of Weibull or Log-normal distribution, both skewed to the left side, to resemble human time performance in control room settings [67,68]. In this work, the Weibull distribution is specified for the task durations for all tasks, with the parameters provided in the task template. The chosen distribution shape parameter resembles human performance for the given task according.

Duration dependence of subsequent tasks is modelled by pair-wise bi-variate distributions. This work uses linear correlation, as the measure of dependence. The bi-variate duration distribution of two subsequent tasks is constructed with the Gaussian copula density c_ρ [69], parametrized with the correction coefficient ρ. The marginal distributions F_1 and F_2 and their densities f_1 and f_2 are the univariate task duration distributions of two subsequent tasks. Given the sampled duration of the first task, t_1, the conditional distribution of t_2 is calculated numerically with the relationship

$$f_{2|1}(t_2|t_1) = \frac{f_{12}(t_1,t_2)}{f_1(t_1)} = \frac{c_\rho(F_1(t_1),F_2(t_2))\cdot f_1(t_1)\cdot f_2(t_2)}{f_1(t_1)} = c_\rho(F_1(t_1),F_2(t_2))\cdot f_2(t_2) \quad (2)$$

Samples are generated *via* a numerical implementation of the inverse-sampling method, using a discretization of one second and a lower and upper bound at the lower and upper 1‰ quantile.

Our approach elicits bi-variate distributions of subsequent tasks, according to Daneshkhah and Oakley [70], with assistance from a Subject Matter Expert (SME). The elicitation process is conducted in three steps:

1) For all task duration distributions, a 3-parameter Weibull distribution with a fixed shape β is chosen, leaving task-specific location μ and scale α to be determined by the elicitation.
2) The SME estimates duration ranges for each successfully executed task type or subtask, which are used as 5% and 75% quantiles to set the location and scale parameters μ and α.
3) The correlation coefficient ρ between subsequent task durations is elicited by asking how likely a task is to take longer than expected, given the previous task has taken already longer than expected [71].

3.3.5. Nominal and alternative mode of operation

To implement the different task duration and HEP conditions for the nominal and alternative mode of operations as described in Section 3.2.5, each task template specifies two sets of parameters for task duration distributions and PSFs. While parameters are set directly for the nominal mode of operation, the parameters for the alternative mode of operations are derived. For the duration distribution, the location parameter μ remains unchanged, as it is mostly defined by technical constraints. The increased execution speed by the human operator is modeled by a 25% reduced scale parameter α with the shape parameter β kept constant. The increased probability of slip errors is determined by increasing the multiplier values of the "Available Time" and "Stress/Stressors" PSFs by one level according to the SPAR-H manual [58]. These increases in PSF multiplier values imply that the operator allows less time for task execution and has a higher perception of stress.

The transition to the alternative mode of operations is only evaluated at pivotal points when a response to a deviation is launched or on the resumption of a plan. Also, upon transiting, the operator will not return to the nominal state. We introduce two transition models, which are a fixed, non-probabilistic transition model and a probabilistic model, built on a Bayesian Belief Network (BBN).

3.3.5.1. Fixed transition model. To determine the transition to the alternative mode of operation, Section 3.2.5 describes operator-specific and external features. To compare the impact of those features, we introduce the fixed transition model which transits to the alternative mode of operation always at the first pivot point observed.

3.3.5.2. BBN transition model. To develop a probabilistic transition model, subject matter expert (SME) judgment is leveraged as available data about the mental state of operators is scarce. Bayesian Belief Networks (BBNs) have been identified as an appropriate modeling tool, allowing to represent complex dependencies while incorporating qualitative and quantitative data from multiple sources, i.e. SME judgment. BBNs have been applied successfully to extend HRA methods and can be built and parametrized based on expert judgment [72]. BBNs are "directed acyclic graphs in which the nodes represent propositions (or variables), the arcs signify direct dependencies between the linked propositions, and the strengths of these dependencies are quantified by conditional probabilities" [73]. This allows for breaking down a joint distribution into its single independent variables and dependence structure, which are parametrized independently.

A BBN is developed to determine the transition probability to the

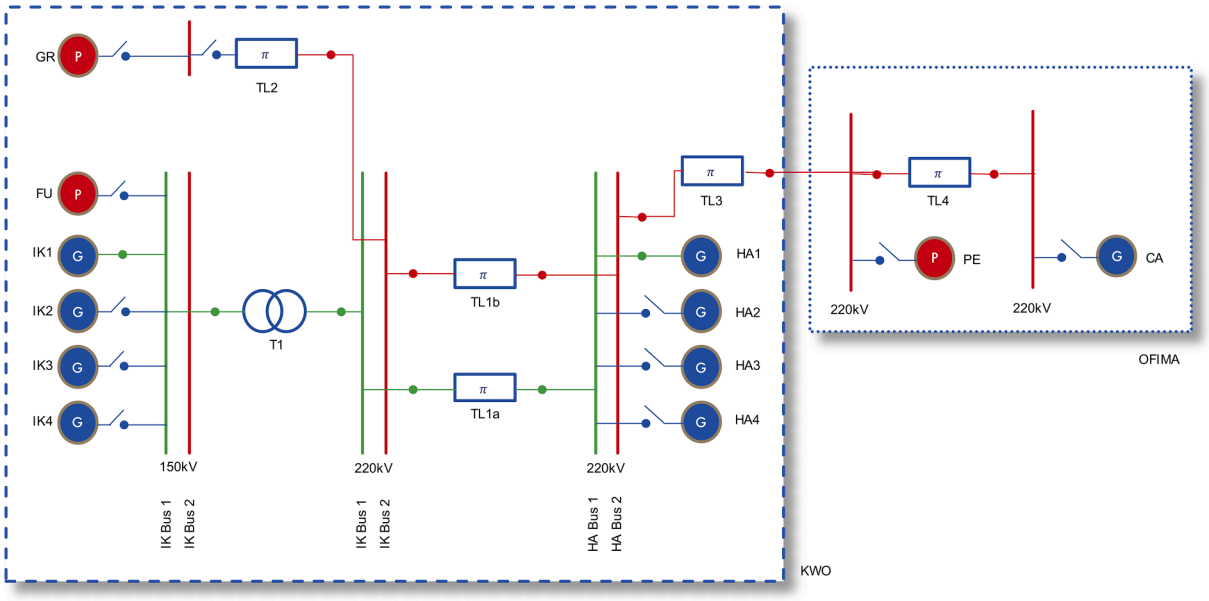


Fig. 4. The joint restoration cell of KWO (dashed) and OFIMA (dotted), in the state after step 3 in the restoration plan.

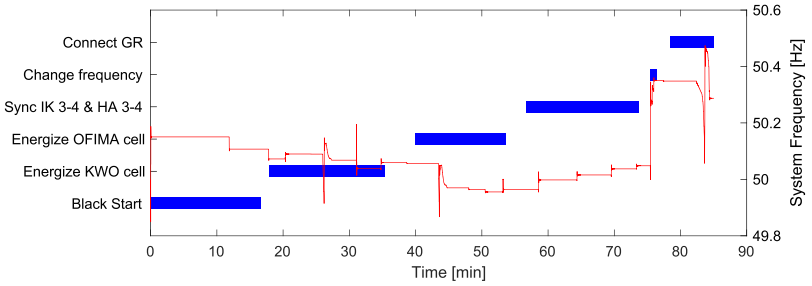


Fig. 5. Six major tasks of the restoration plan (left axis) and their duration (bars) with an overlay of the frequency transient (right axis). The frequency is controlled to 50.15 Hz in the beginning and increased to 50.35 Hz before connecting the Grimsel pump to avoid triggering of pump disconnection thresholds.

alternative mode of operation at pivotal points and apply its sampled outcome. The transition probability depends on external and operator-specific features. While operator-specific features are assumed to be constant for a given operator throughout the whole operation, external features may depend on the system state or the elapsed time and are subject to change. Based on interaction with stakeholders in the power grid operations domain, we propose three relevant features for a BBN: (1) The inclination to change to the alternative mode of operation has been identified as an operator-specific feature and is assumed to be constant for a given operator; (2) The time until the start of the cold load effect [74] – the change of load characteristics, particularly of residential loads – da is a dynamic external feature; (3) The perceived urgency is an operator-specific intermediate state, while the dependent outcome is the transition to the alternative mode of operation. This structure is illustrated in Fig. 3, where green boxes represent independent stochastic variables, orange boxes represent external dynamic variables, and blue boxes represent conditional probabilities. The variable "inclination to change operations" is drawn only at the first pivotal point and remains unchanged thereafter. "Perceived urgency" is sampled based on the time left until the start of the cold load effect.

4. Case study

In the national power grid restoration plan, which is part of an emergency response strategy, restoration cells build the basis of Swissgrid's bottom-up restoration strategy [47]. In the process of designing a national high-level restoration plan [47], which covers the further phases of re-energization, re-synchronization and load-pickup, the timing and availability of restoration cells is crucial. This case study demonstrates how to evaluate a restoration cell regarding its availability and performance to draw conclusions about its suitability in a higher-level restoration plan.

The case study investigates the joint restoration cell of KWO and Officine Idroelettriche della Maggia (OFIMA) [75], where KWO takes the role as lead operator. Its restoration process' performance and resilience is assessed in terms of duration and human failure. KWO conducts live restoration exercises for its operators every two years which focus on technical challenges in the restoration process, such as transient stability or inrush currents. However, this joint cell was only practiced once. In addition, simulator exercises are used to train the operators on restoration plans and procedures under time pressure and under realistic staffing conditions. Since live and simulator exercised only examine a limited number of scenarios, this case study demonstrates the capability to investigate an extensive range of possible evolutions within a plan. This case study simulates two scenarios: A baseline, addressing the planned execution of the restoration plan and a disruption scenario, aiming to determine the implications of spurious tripping and maintenance errors.

4.1. Restoration cell and restoration plan

Fig. 4 shows the joint restoration cell. The dashed area shows the part belonging KWO, while the dotted area indicates the part belonging to OFIMA.

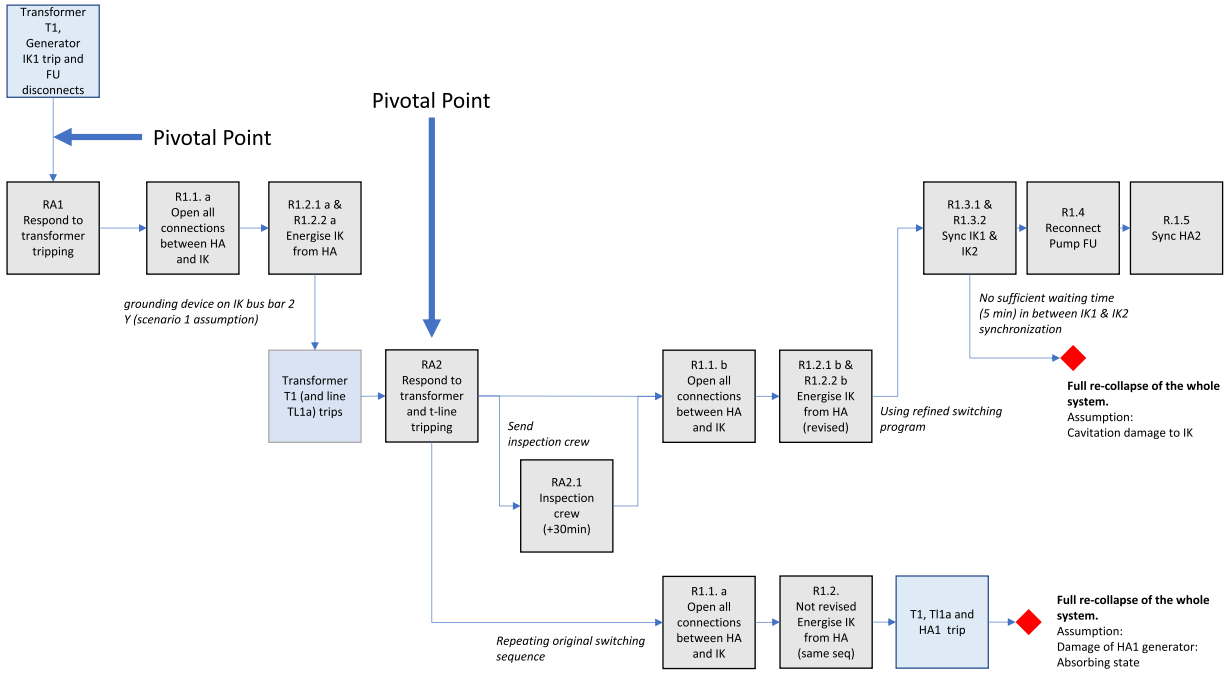


Fig. 6. Event-sequence diagram of the scenario.

KWO has full switching permission on all components *via* SCADA and all operations are coordinated from the KWO's control room in Innertkirchen (IK, in Fig. 4). The power plants in IK and Handeck (HA) have four generators each and are black start-capable; that is, the restoration has to be initiated either from IK or HA. The preferred high-level restoration plan is executed in 23 steps and is listed in Appendix 5. The milestones of one realization are shown in Fig. 5 as a task progression (left y-axis) with an overlay of the system frequency (right y-axis), which is calculated in simulation runtime *via* a phase-lock-loop from the three phase bus voltage in IK.

With black-starting one generator in IK (Black Start), the set frequency is set at 50.15 Hz to ensure sufficient leeway to the disconnection thresholds of pumps. The KWO cell is energized (Energize KWO cell), covering the switching of transmission line TL1 to HA and synchronizing two generators in HA and one additional generator in IK to gain more inertia. Subsequently, the Fuhren pump (FU) is connected to provide a load for the four generators, resulting in a transient of 0.2 Hz magnitude. The plan proceeds from this stable KWO cell to energize the OFIMA cell by switching transmission line TL3 over the Alps. At this stage, the OFIMA cell is energized, starting with the connection of the Peccia pump (PE) and followed by the switching of TL4 and synchronization of the power plant in Cavergno (CA). For the next milestone, the remaining four generators in HA and IK are synchronized (Sync IK 3-4 & HA 3-4). Before finalizing the process, the frequency is increased to 50.35 Hz (Change frequency) to avoid triggering protections due to the resulting transient of 0.7 Hz magnitude. The plan concludes with the connection of the pump in Grimsel (Connect GR). It can be observed from the frequency that particularly the change of frequency and connection of GR cause more significant transients, a potential cause of tripping due to over- or under-frequency protections if target frequencies are not met.

4.2. Scenarios

4.2.1. Baseline scenario

The baseline scenario of this case study simulates the restoration plan provided in Section 4.1 and represents the best practice. Its main aim is to demonstrate the application of the developed model and to determine those steps particularly prone to failure. In the discussion of the baseline scenario, the alternative mode of operations is evaluated.

4.2.2. Disruption scenario

The disruption scenario aims to demonstrate the capabilities of the model to handle complex, modified scenarios with unanticipated errors and additional responses to the resulting deviations. Two specific anomalies are added to the baseline scenario following interaction with Swissgrid. The first anomaly is a spurious tripping of the transformer in the early stage of re-energization. This effect has been observed before, particularly for inrush currents and transients when components and their protection mechanisms operate far below their usual operating points.

Components that have not been in use after the conclusion of maintenance works might be part of a restoration plan or responses, increasing the impact of maintenance errors. Hence, the second anomaly of the scenario is the presence of a physical earthing device that has been left behind on a bus bar by a maintenance crew, not detected before releasing the bus bar for operations, and not visible in SCADA.

The disruption scenario unfolds as illustrated in Fig. 6:

- The FU pump connection's power flow transient causes the transformer T1 to trip. Consecutively, two disconnected islands – IK and HA – are formed. The IK Island trips as its inertia cannot damp the still unfolding frequency transient caused by the pump connection.
- The operator may assess the situation (labeled as RA1 in Fig. 6) and decide on the execution of response R1a. When completed, it would allow the resumption of the main restoration plan in step 8. When re-energizing the IK island, the operator will choose the second bus bar on the 138 kV level in IK for the connection of the transformer in step R1.2a. This bus bar is un-knowingly still equipped with a physical earthing device, leading to a repeated tripping of T1 and TL1a.
- After the repeated tripping of T1 and TL1a, the operator assesses the situation (labeled as RA2 in Fig. 6); a successful outcome detects the grounded bus bar as the cause. In this case, the operator selects the first bus bar instead and re-performs the modified response R1b. In the unsuccessful outcome, the operator interprets the tripping as a

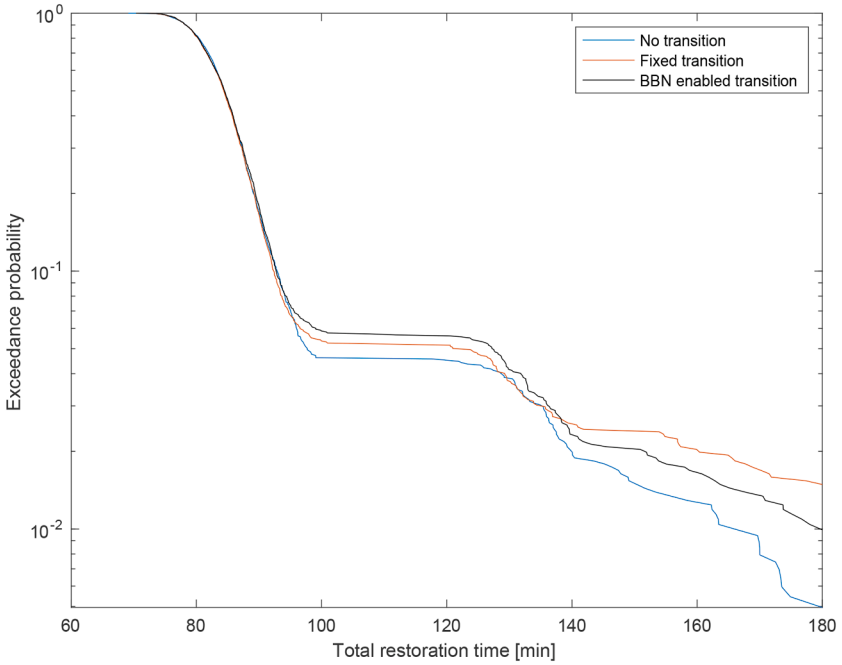


Fig. 7. Restoration duration exceedance probability under all three assumptions.

voltage management issue and repeats the switching to the second bus bar on the IK 138 kV level. In that case, it is assumed that the effects of this second short circuit switching damage the HA generator shaft.

- In the case of a successful proceeding beyond R1.2, two generators of IK are to be synchronized in order to increase the locally available inertia and power reserve. However, if two generators within the same hydro-plant are synchronized, at least 5 min need to pass between the synchronization to allow for the hydro-dynamics to settle. A premature synchronization with less than 5 min in between R1.3.1 and R1.3.2 might thus lead to cavitation damage of the IK plant.

4.3. Metrics

The re-energization of a cell is conducted in an isolated system over less than 2 h. As the cell does not serve any other loads during its energization, there is no measure of performance or economic impact varying through this time. Hence, metrics such as the resilience curve [76] and its derived integrated loss of service [10] render unsuitable. Since the topology and components of the cell is fixed, its impact for the further TSO high-level restoration plan is determined by its design. Hence, the most critical metrics of the cell derive from its total restoration duration and its availability. Since both features directly depend on human performance, we propose to use the exceedance probability of total restoration times and the probability of non-availability, either due to excessive delays beyond 3 h or component damage.

4.4. Determination of error probabilities: performance shaping factors

For every task or sub-task explicitly modeled, either a scenario error or task error is defined. To derive the human error probability (HEP) for each task, Appendix 2 lists the SPAR-H task type and PSF multipliers for all relevant human failure events of tasks and sub-tasks.

In this study, the crew is modeled as one operator. Hence, average values for PSF multiplier values are estimated. Further, only one set of PSFs is used, i.e. PSFs do not vary among crews. PSFs were chosen and multiplier values were assigned based on existing literature, observations of a live exercise at KWO, and engineering judgment. Abreu et al. [66] evaluated the HEP for the emergency switching of a transmission line based on the PSFs available time (barely adequate, 10), complexity (moderately complex, 2), and work processes (good, 0.8). Shuvro et al. [31,32] and Wang et al. [33] assessed the human performance within an unfolding cascade *via* simulation and assigned the multiplier for the PSFs available time, stress, and complexity dynamically based on the system state. Zhou et al. [34] investigated a dispatching task which was decomposed into a diagnosis and action sub-task. For the diagnosis task, the PSFs chosen were available time (nominal, 1), stress (extreme, 5), complexity (high, 5), experience/training (nominal, 1), ergonomics/HMI (nominal, 1), and work processes (incomplete, 20). For action, respectively, the PSFs were available time (time available $\geq$ 5x the time required, 0.1), training (nominal, 1), and work processes (good, 0.8). Those PSFs and their multiplier values were considered as reference, while accounting for differences in the specific tasks and the circumstances during restoration.

In the case of restoration, tasks follow the restoration plan that has been designed with a given target duration. Further, the stress level can be assumed to be also at a constant level across all tasks that take place within the plan. However, as argued in Section 3.2.5., an operator that experiences a deviation to the plan might transit to the alternative mode of operations with an elevated level of stress while allowing less time for the execution of tasks. Hence, we choose the PSFs available time and stress as dynamic PSFs while treating all other PSFs as static.

The PSF for complexity of all tasks is set as moderately complex as tasks require more mental steps than in normal operations due to the increased share of control actions performed by the operator. Further, the PSF stress / stressors is set as high to reflect the general conditions during restoration. The alternative mode of operations model affects the available time and stress PSFs by an increase of one level according to the SPAR-H manual [58]. All crews consist of two operators with at least of one member with sufficient experience, hence we set the PSF for experience to a nominal level. The HMI and ergonomics are judged as suitable for the restoration process and hence also with a nominal value. Due to a lack of knowledge, the PSFs for procedures, fitness for duty, and work processes are not assigned.

4.5. Duration distributions

The duration distributions are elicited according to Section 3.3.3

Table 2
Statistics for all scenarios. Quantile values of successful restorations and the share of simulations containing deviations, exceedance of 180 min or fail due to component damage.

Operations model	Quantiles [min]			Simulations with deviations [%]
	50%	90%	95%	
No transition	84	93	98	4.71
Fixed transition	84	92	121	5.36
BBN-enabled transition	85	93	127	5.9

from one SME and validated from one restoration exercise observation. The SME has over 20 years of experience planning and supervising simulator exercises and live exercises conducted in restoration cells. The shape for all tasks has been set to $\beta = 1.8$. All distributions were validated, determining if observed exercise durations are within one standard deviation. Between two consecutive tasks, the correlation coefficient is estimated as $\rho = 0.5$ and $\rho = 0$ for tasks, which are executed subsequent to a pivotal point, i.e. at the start or end of a deviation. The detailed distribution parameters are listed in Appendix 3.

4.6. Human operator modes of operations

Three different configurations for the mental mode of operations shall be assessed. First, two boundary cases are simulated, with one model executing all tasks strictly in the nominal mode of operations without transitioning to the alternative mode, labeled as "no transition". In the other boundary case, a transition to the alternative mode of operations always occurs at the first observed pivotal point. The simulation conducted under this assumption is labeled as "fixed transition" and does not consider any operator or dynamic external features.

The case labeled as "BBN enabled transition" utilizes the BBN structure introduced in Section 3.3.5. The probabilities and conditional probability tables which have been set by engineering judgment are given in Table 5, Appendix 3. The dynamic external factor is set as the time left to the cold load effect [74] which is estimated to gradually come into effect after 90 min into the blackout. The time left until the deadline is indicated by T_D, while the threshold t_D influences the probability of perceived urgency and is set to $t_D = 10$ min. The inclination to change operation is assumed with a probability of 0.5 to be either high or low. The conditional probability tables for the perceived urgency and transition to the alternative mode of operation are shown in Tables 6 and 7, Appendix 4.

5. Results and discussion

First, the baseline results are established and their sensitivity regarding the alternative mode of operation is analyzed. In the second part, we introduce the disruption scenario to demonstrate the analysis of errors, deviations and dominant contributors. All simulations of the baseline scenario are carried out with a sample size of $N = 2016$. The disruption scenario sample size is chosen $N = 3024$ in order to cover the increased number of absorbing states. The simulation of both scenarios is carried out until a maximum simulated time of 180 min, after which restoration fails.

5.1. Baseline scenario

The results of the baseline scenario have been computed under the three operations models presented in Section 4.6. and are shown in Fig. 7. The boundary conditions are established by the case of no transition (plotted in blue) and the case which assumes a fixed transition at the first pivotal point (plotted in red). The model with the BBN-enabled transition is plotted in black. Table 2 summarizes the quantile values, share of simulations with deviations, and the estimated probability of exceeding 180 min. All curves show a similar pattern: The first decay in exceedance probability comprises the time of normal restorations without any deviations. A significant gap in exceedance probability only widens beyond 92 min which corresponds to 8% exceedance probability. Ultimately, 180 min are exceeded with a probability of 0.5% in the case of no transition, 1.5% with the hypothetical fixed transition and 1% with the BBN enabled transition model. All approaches estimate a similar time performance but differ in the tail, adding additional insight for risk management purposes.

To explain the shape of the exceedance curves in the case of deviations, Fig. 8 puts into relation total restoration time and time spent within deviations. To account for the fact that an operator might change to the alternative mode of operation, the dataset of the BBN-enabled transition has been chosen which consists of 119 samples containing deviations. In the dataset provided, those samples cover the whole tail

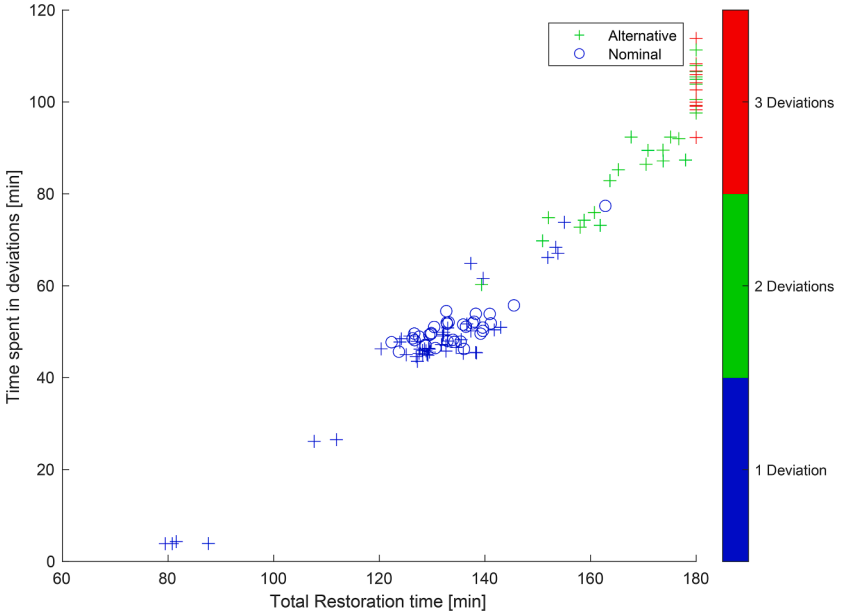


Fig. 8. Comparison of all 119 samples in the BBN-enabled operational model which contain deviations regarding duration spent during deviations and number of deviations.

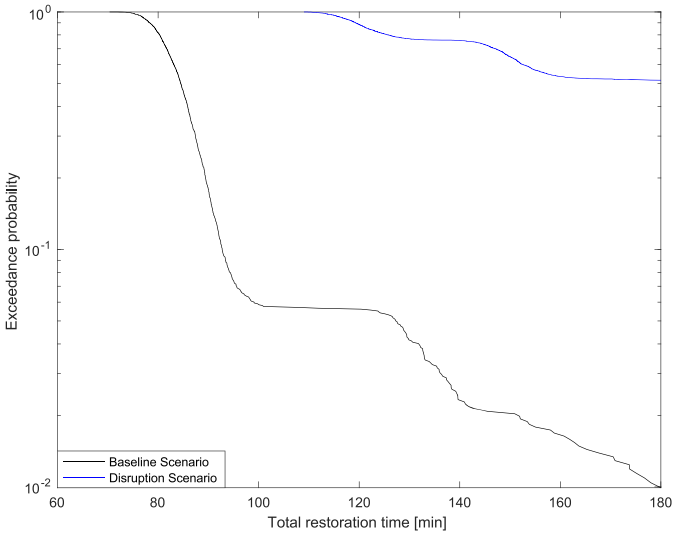


Fig. 9. Unconditional exceedance plot of successful restorations. Comparison of the disruption scenario (blue) and the baseline scenario (black). In the disruption scenario, only 52.5% of all samples lead to a successful restoration.

beyond 101 min. Among those samples, it is further distinguished if samples contained one, two or three deviations and if the alternative mode of operation is observed. Only 4 samples, corresponding to 0.2%, are below the 90% quantile of all samples, and the number of deviations and, thus, the time spent in deviations increase the total restoration time. All samples which contain three deviations exceed 180 min. Furthermore, samples with no alternative mode of operation invoked only contribute 28.6% and contain a maximum of one deviation. This can be interpreted in two directions: A higher number of deviations increases the probability of transitioning, while under the alternative mode of operations, the HEP and thus the likelihood of deviations increases.

5.2. Disruption scenario

Following the event-sequence diagram in Fig. 6, component damage is now a potential outcome due to human errors. Thus, a total of three outcomes need to be accounted for: 52.5% of all samples lead to a successful restoration, component damage accounts for 38.29% of all samples, and 9.16% exceed a restoration time of 180 min. The resulting unconditional exceedance probability plot of the disruption scenario's successful restoration is plotted in Fig. 9. For reference, the baseline exceedance probability plot for the baseline scenario is plotted in black. As a consequence of the scenario-events and scenario errors, a delay of at least 39 min in the 25% quantile is observed.

Fig. 10 shows one sampled restoration for the disruption scenario, leading to a successful outcome but containing one additional deviation and overlays the frequency transient and task progression diagram. Tasks part of the restoration plan are marked as P, tasks part of the scenario as RA or R,1 according to Fig. 6, and responses to further deviations as R. As the scenario contains one grid split, the system frequencies in Innertkirchen and in Handeck are plotted.

At the connection of the FU pump the disruption scenario starts and the spurious tripping of the transformer causes the grid split and the IK side collapses. In RA1, the operator chooses bus the 150 kV bus bar 2 in the re-energization of the IK side, which is affected by a maintenance error, leading to another tripping. In response, the operator decides in RA2 against sending an inspection crew and concludes rightfully to use bus 1 instead. The cases with an additional 30 min delay due to the sending of an inspection crew are reflected by the flatter shape of the exceedance plot in Fig. 10 and the increased probability of exceeding 180 min.

The original restoration plan is resumed after 70 min with the switching of the transmission line between HA and PE. After 101 min, a failure to set the frequency correctly leads to a frequency disconnection of two generators and the PE pump, causing a drawback of 11 tasks. After 157 min, the restoration concludes successfully.

5.2.1. Analysis of dominant contributors

Table 3 summarizes those tasks which contain errors, and lead to

Table 3
Contributors to deviations and errors and damages; Total size of the dataset N = 3024.

Task	Deviations	Errors	Deviation caused by error	Other deviations
Connect FU	Given by	133	Given by scenario	
Switch T1 on Bus 2	scenario	0		
Set frequency	496	204	199	297
Connect GR	54	130	54	0
Connect PE	3	175	2	1
Sync CA	1	21	1	0
Sync others	0	144	0	0
Situation assessment of RA2	0	1090	0	0

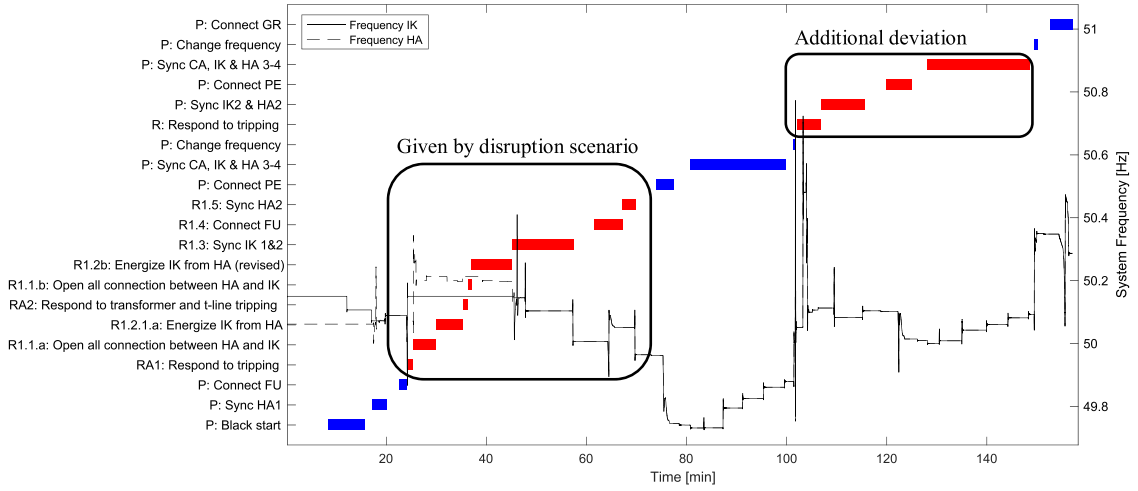


Fig. 10. Frequency transient and task progression of the disruption scenario. The plotted realization shows the deviation given by the disruption scenario and also contains one additional deviation. Tasks which are executed according to the plan are plotted in blue, off-plan deviations or repeated tasks are plotted in red.

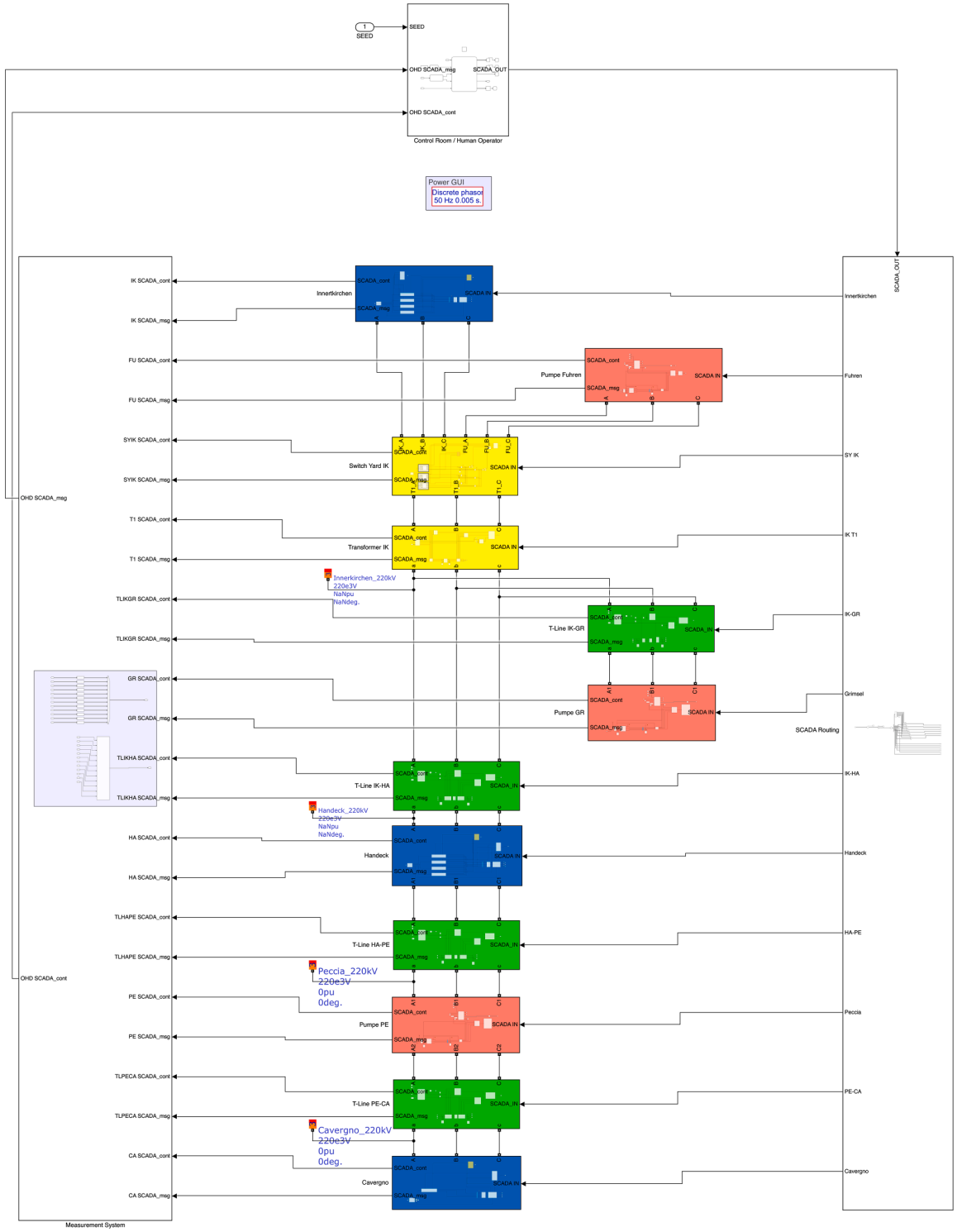


Fig. 11. High-level view of the extended cell implemented in Simulink. Signals between A/a, B/c, and C/c ports represent electrical connections. Other signals with an arrow represent SCADA messages and continuous measurements. Power plants are colored in blue, pumps in red, transmission lines in green, and switchyards or transformers are colored in yellow.

deviations or damage. Further, it shows how many errors within the task caused an immediate deviation, and the number of deviations that occurred immediately after the task despite no error within the task. The deviations after connecting the FU pump and the switching of the transformer T1 on bus 2 occur in all 3024 samples as they are given by the scenario input. Additionally, the repeated switching of the transformer on bus 2 results in 1090 damages, which can be directly connected to the same number of errors observed in the situation assessment in RA2. Among the deviations not defined by the scenario input, the change in set frequency is a dominant contributor. More than half of those deviations occur despite no error within the task. This can be explained by errors in previous tasks, either changing the transient

Table 4
Task-based and scenario-based errors, task types, action (A) or diagnosis (D), and PSF multiplier values assigned in the normal mode: Available Time (A), stress (S), complexity (C), experience/training (Ex), procedures (P), ergonomics and HMI (Er), fitness for duty (F), work processes (W).

Task Task-based errors	Error	Type	A	S	C	Ex	P	Er	F	W
Synchronize generator: Assess and start synchronization	Premature synchronization, causing cavitation damage	D	1	2	2	1	1	1	1	1
Synchronize generator: Correct transient	Over-correction of frequency transient	A	1	2	2	1	1	1	1	1
Connect pump	Over-correction of frequency transient	A	1	2	2	1	1	1	1	1
Change frequency Scenario-based errors	Increment too high	D	1	2	2	1	1	1	1	1
Situation assessment (identification of the physical earthing device, disruption scenario RA2)	Non identification	D	2	1	5	1	1	1	1	1

Table 5
Task duration ranges and derived parametrization for the Weibull distribution with location **μ**, scale **α**, and shape **β**.

Task	Min [s]	Max [s]	**μ**	**α**	**β**
HMI parameter setup (restoration preparation, per sub-task)	30	90	16	63	2
Black start generator	150	500	135	368	1.8
Synchronize generator	180	300	151	126	1.8
Connect pump: Prepare connection (check conditions)	120	360	63	252	1.8
Connect pump: Connection	60	180	31	126	1.8
Connect pump: Correct frequency transient	120	420	90	315	1.8
Switching of components	60	180	31	126	1.8
Adjustment of frequency	180	300	151	126	1.8
Situation assessment	120	450	41	347	1.8
Re-planning	180	450	116	284	1.8

Table 6
Conditional probability for perceived deadline urgency DU, referring to the time T_D until the cold load effect (90 min). The threshold of 10 min is indicated as t_D.

Time until deadline T_D	Probability of perceived urgency DU
$T_D > t_d$	0.05
$0 < T_D \leq t_D$	0.5
$T_D \leq 0$	0.9

Table 7
Conditional probability table for transitioning to the alternative mode of operation, given low or high inclination to change operation and perceived deadline urgency.

Inclination to change	Perceived deadline urgency	Probability of transiting to alternative mode of operation $P(AO)$
Low	False	0.1
Low	True	0.7
High	False	0.5
High	True	0.9

due to different system behavior or due to an insufficient frequency margin. Thus, it is indeed possible that errors in previous tasks do not have immediate negative consequences but might come into effect later. The system does also, dependent on its frequency reserve, tolerate error outcomes. This can be observed at the connection of the Grimsel pump in task 23 which concludes the plan successfully, if no deviations occur. In total, out of 130 observed errors, only 54 lead to deviations.

While deviations result in delays, component damages may render a restoration cell unavailable, which makes their coverage crucial to the risk management of a TSO. The two contributors to component damage, causing failure of the cell, are the repeated switching of the grounded bus bar, and the premature synchronization of the second generator in IK, causing cavitation damage to the plant. Repeated switching is hereby the dominant contributor to component damage: The high number of 1090 out of 1158 damages in 3024 simulations can be explained by the high share of situation assessment errors which lead to the repeated switching. The lower number of 68 damages attributing to premature synchronization is caused by the fact that in most cases, the time between two synchronizations exceeds 5 min, which would lead to such damage.

Table 8
Restoration plan for the joint cell.

Step	Task type	Target /Value	Step	Task type	Target /Value
1	Switch bus 1	IK 138 kV	**13**	Connect pump	PE
2	Switch transformer	T1	**14**	Switch transmission line	TL4
3	Switch transmission line	TL1a	**15**	Switch plant breaker	CA
4	Switch plant breaker	IK	**16**	Synchronize generator	CA
5	Black start generator	IK 1	**17**	Synchronize generator	IK 3
6	Switch plant breaker	HA	**18**	Synchronize generator	HA 3
7	Synchronize generator	HA 1	**19**	Synchronize generator	IK 4
8	Switch pump	IK 138kV	**20**	Synchronize generator	HA 4
9	Connect pump	FU	**21**	Change set frequency	50.35 Hz
10	Synchronize generator	IK 2	**22**	Switch transmission line	TL2
11	Synchronize generator	HA 2	**23**	Connect pump	GR
12	Switch transmission line	TL3			

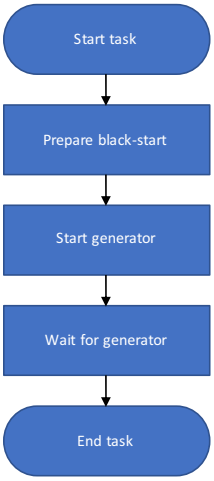


Fig. 12. Black start task.

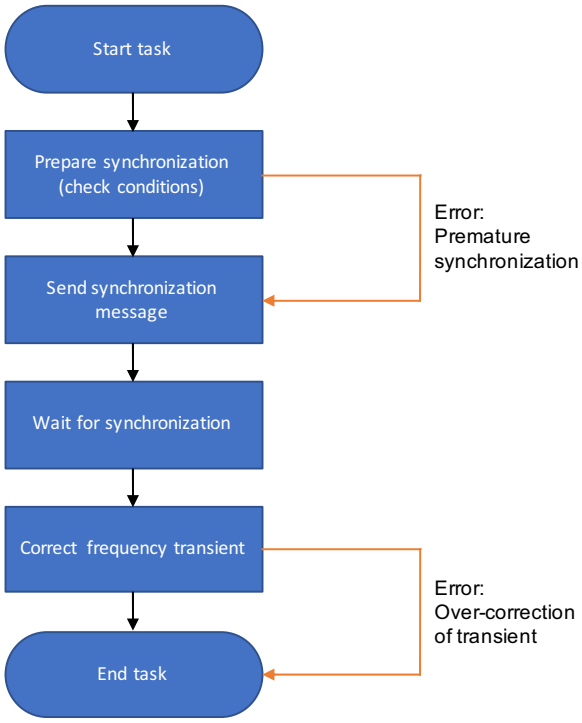


Fig. 13. Synchronization task.

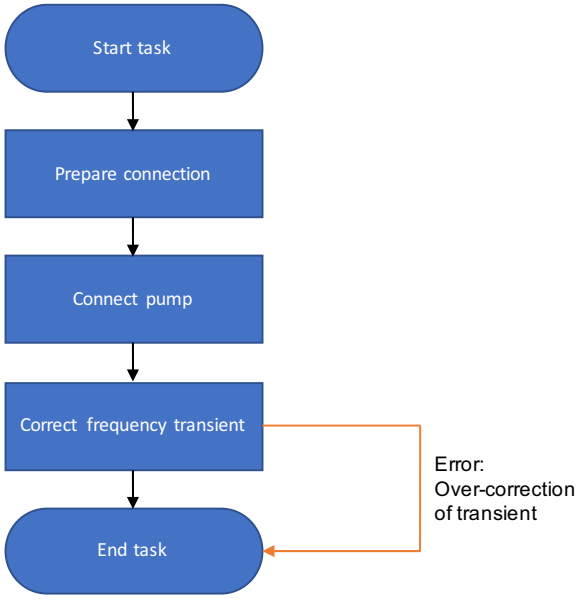


Fig. 14. Pump connection task.

5.3. Insights and practical recommendations

Major takeaways from the case study address the prioritization of trained responses, and perspective restoration time. All samples exceed a normally desired time of 30–60 min and the probability of the cold load effect is estimated at above 25%, which raises the question if this cell should be reduced in size. Alternatively, this cell might be planned to join later stages of the re-energization instead of building its basis. Further, the design of responses becomes critical as operators only train a limited set of responses, covering all possible deviations.

The high share of deviations after the change of set-frequency task raises particularly two important points. First, the system behavior might change due to previous errors, potentially resulting in an unexpected system response even if the task is performed correctly. Second, the system is capable to tolerate errors to a certain degree due to a frequency margin. Hence, a thorough frequency planning should be performed when designing a restoration plan, accounting for potential human when budgeting the frequency margin.

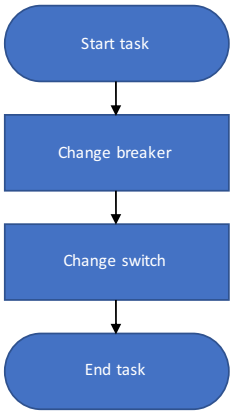


Fig. 15. Switching task.

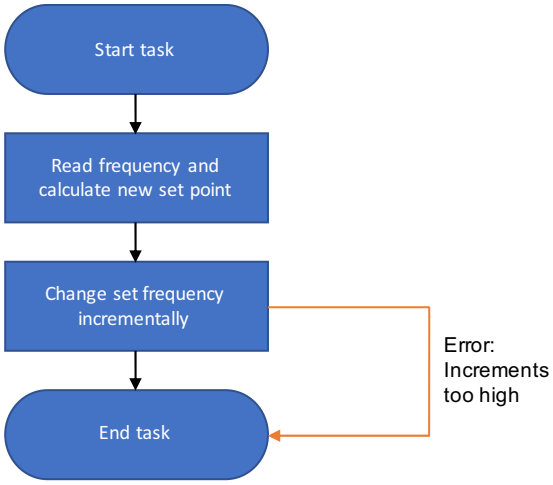


Fig. 16. Adjustment of frequency task.

5.4. Further discussion

5.4.1. Limitations of the validation

While preparing this study, one restoration exercise of KWO in the autumn of 2021 was attended with a total duration of 65 min, while the expected value of the same scenario, generated with the model presented is 70 min. However, the sparsity of currently available recorded data limits the validation to SME and human factors expert-based approaches. Exercises are currently the only source of observations but do not precisely resemble the realistic restoration conditions after a blackout regarding equipment availability and staffing. The literature shows only limited comparable studies and previous work focusing on the duration distribution without considering human errors and deviations [12,13]. Further, those studies employing HRA methods in the domain of power grid operation do not focus on restoration and do not look at the duration [32,34,66]. Thus, no comparable study was available which could serve for validation. However, the combination of SME elicitation, available publications, and observed exercises enables the estimation of the distribution of restoration times and outcomes of errors. This estimation is sufficient to draw the conclusions mentioned in Section 5.3.

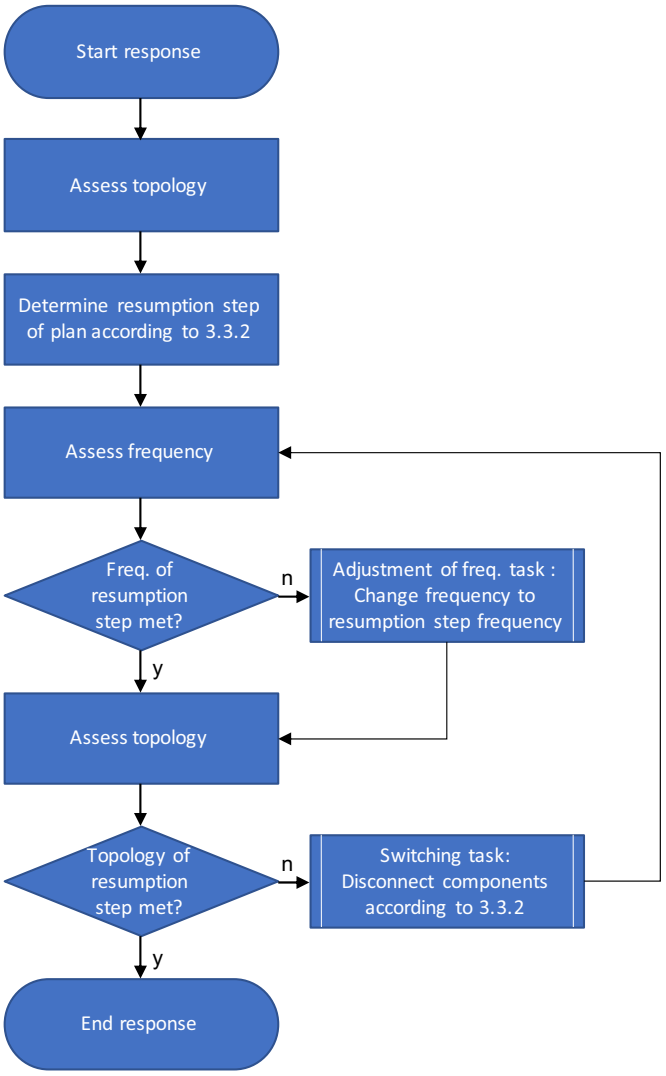


Fig. 17. Response to failures. Boxes with double lines indicate other tasks as sub-routines.

5.4.2. *Limitations of the case study and models*

The crew has been modeled as a single-operator model, which is justified in this application because a single operator has the decisional responsibility for all tasks in the restoration cell. While this simplification is valid for most of the described tasks, it does not fully capture the crew effort during the situation assessment after component tripping and deviations. Further, if the developed model shall be employed for the further steps in the restoration process, e.g. re-synchronization, multiple operator models would be required as well as the model of their communication.

As outcomes and errors are identified in the HTA, any other errors and outcomes or unexpected situations are not covered in this case study. Further, the use of task templates in the operator model restricts the variety of errors, only considering slips and mistakes. However, lapses and more refined planning mistakes are not included in the case study at this stage. Furthermore, the operator can only apply those responses which have been included in the model but are not able to derive knowledge based responses.

The power grid model used in this simulation was developed to resemble the equipment characteristics with all available parameters based on standard models from the Simscape library. As a result, the grid model does not precisely resemble the behavior of power plants, pumps, transmission lines, and transformers, particularly their frequency transients and inrush-currents. However, a higher fidelity model of the power grid is not expected to change the conclusions substantially since the effects do not have significant impact on the bulk of the distribution without errors.

6. Conclusion and future work

Our approach enhances the state-of-the-art by presenting a full operator model for power grid operations, considering human performance in terms of task durations and human failure events. The model has been implemented in MATLAB Simulink, and its capabilities were demonstrated in a case study of a restoration cell.

The simulation framework presented, involving the operator-grid model and the execution of plans, gives a tool for efficiently assessing procedures, improving plans, and prioritizing response training. Further contributions are the postulated alternative mode of operations model, which has been developed into the model. Our approach employs a BBN to derive the conditional probability of a change of state of an operator's mind, given external inputs such as time to deadlines and operator-specific factors, such as their inclination to change operation.

For those approaches focusing on human contribution to system stabilizing in cascades, one potential application in current research is to compare different strategies from a set of trained responses. Our approach provides a plan and response-driven framework to assess related operations concerning the restoration capacity. Enhancing state of the art, we have proposed using task templates instead of hard-coded tasks for task executions as part of plans, procedures, and responses.

For governments, the prediction of restoration time supports community information, risk management of critical infrastructure, and the business continuity planning of other stakeholders. TSOs, DSOs, and GenCos involved in the emergency response also may enhance their risk management by employing simulation-based assessment of restoration operations. Risk management for over-time and non-availability of a restoration cell allows for a more resilient design of higher-level TSO restoration plans. Therefore, pre-assessment of measures will enable the comparison of different options and allow better budgeting for the human contribution to risk and performance. The prioritization and training of responses may be mainly supported by identifying the most likely deviations and choosing those responses yielding their best coverage.

The power industry further might identify dominant contributors to delays or non-availability in operations through the combination of HTA and simulation. Those insights may support prioritizing the training of tasks and even – if possible – prioritizing their automation.

Future work might mainly address the validation of the model through data collected during simulator and live exercises, lab experiments, or extended SME elicitations. Notably, the data quality on duration distributions and their dependence needs improvement. PSF multiplier values should be evaluated by trained SPAR-H experts and potentially enhanced with lab experiments, such as discussed by Zhou et al. [34]. The postulated alternative mode of operation might be further investigated through structured SME interviews and lab experiments to verify its exact features.

Task templates for further tasks of the restoration process, such as voltage management or the re-synchronization tasks, should be developed. Situational awareness should be incorporated into the operating model to unlock the potential of previous results from research on cognitive tasks. Task templates might be further translated from HTA and domain analysis into ACT-R models, as suggested by Li and Blanc [29], to leverage existing research in cognitive science and work psychology. The planning of responses may also be further investigated to resemble the on-spot drafting of responses by human operators more realistically.

CRediT authorship contribution statement

Felix Kottmann: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Visualization. **Miltos Kyriakidis:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Supervision. **Giovanni Sansavini:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Supervision. **Vinh Dang:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of Competing Interest

No conflicts of interests are known.

Data availability

The data that has been used is confidential.

Acknowledgments

This work was supported by the Future Resilient Systems Programme under the Singapore-ETH centre.

We would like to thank Dr. Walter Sattinger and Dr. Asja Derviškadić of Swissgrid who took the time to provide an overview of an operations center and its inner workings, provided insight and expertise that were essential to this research, and made possible the observation of a restoration exercise.

The views expressed in this article are those of the authors and do not necessarily reflect those of Swissgrid.

Appendix.

1. *Human operator – power grid system*

   Fig. 11.

2. *PSFs for the tasks part of the case study*

   Table 4 shows task with error outcomes, the SPAR-H task type and PSF multiplier values.

3. *Task duration distribution parameters*

   Table 5 shows the elicited range (Min, Max) for tasks and sub-tasks and the calculated parameters for the Weibull distribution.

4. *Alternative mode of operation: conditional probabilities*

   Table 6 shows the conditional probabilities for the perceived urgency with T_i the time left until a deadline, t_i the according threshold. Table 7 shows the conditional probabilities to transit to the alternative mode of operation.

5. *Restoration plan*

   Table 8.

6. *Flow charts of tasks*

Black start
Fig. 12.

Synchronization
Fig. 13.

Connection of pumps
Fig. 14.

Switching
Fig. 15.

Adjustment of frequency
Fig. 16.

Response to failures
Fig. 17.

List of abbreviations

BBN	Bayesian Believe Network
CA	Cavergno (Generator location in Switzerland)
DSO	Distribution system operator
ENTSO-E	European Network of Transmission System Operators for Electricity
FU	Fuhren (Pump location in Switzerland)
GenCo	Generation System Operator
GR	Grimsel (Pump location in Switzerland)
HA	Handeck (Generator location in Switzerland)
HEP	Human Error Probability
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
HVDC	High Voltage Direct Current
IK	Innertkirchen (Generator Location in Switzerland)
KWO	Kraftwerke Oberhasli (Generation system operator in Switzerland)
OFIMA	Officine Idroelettriche della Maggia (Generation system operator in Switzerland)
OHD	Overhead display
PSF	Performance Shaping Factor
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
TSO	Transmission System Operator

References

[1] Dierick, M., et al., Continental Europe synchronous area separation on 24 July 2021. 2021, ENTSO-E: https://eepublicdownloads.azureedge.net/clean-documents/SOC%20documents/SOC%20Reports/entso-e_CESysSep_210724_211112.pdf.

[2] Reyer, F., et al., Continental Europe synchronous area separation on 08 January 2021. 2021, ENTSO-E: https://eepublicdownloads.azureedge.net/clean-documents/SOC%20documents/SOC%20Reports/entso-e_CESysSep_Final_Report_210715.pdf.

[3] Kenward, A. and Raja U., Blackout: extreme weather climate change and power outages. 2014, Climate central: https://assets.climatecentral.org/pdfs/PowerOutages.pdf.

[4] Krämer, C. Switzerland was on the verge of a blackout. 2019 10.06.2019 [cited 2022 19.10.2022]; Available from: https://gridradar.net/en/blog/post/switzerland-was-verge-blackout.

[5] Al Masood N, Yan R, Saha TK. Cascading contingencies in a renewable dominated power system: risk of blackouts and its mitigation. In: Proceedings of the 2018 IEEE power & energy society general meeting (PESGM). IEEE; 2018.

[6] Ton DT, Wang WP. A more resilient grid: the US department of energy joins with stakeholders in an R&D plan. IEEE Power Energy Mag 2015;13(3):26–34.

[7] National Academies of Sciences, Engineering, Medicine. Enhancing the resilience of the nation's electricity system. Washington, DC, USA: National Academies Press; 2017.

[8] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures. Reliab Eng Syst Saf 2017;157:35–53.

[9] Van Hentenryck P, Coffrin C. Transmission system repair and restoration. Math Program 2015;151(1):347–73.

[10] Kottmann F, et al. Enhancing infrastructure resilience by using dynamically updated damage estimates in optimal repair planning: the power grid case. ASCE-ASME J Risk Uncertain Eng Syst Part A Civil Eng 2021;7(4):04021048.

[11] Xu N, et al. Optimizing scheduling of post-earthquake electric power restoration tasks. Earthq Eng Struct Dyn 2007;36(2):265–84.

[12] Abbaszadeh A, Abedi M, Doustmohammadi A. General stochastic Petri net approach for the estimation of power system restoration duration. Int Trans Electr Energy Syst 2018;28(6):e2550.

[13] Mota AA, Mota LTM, Morelato A. Visualization of power system restoration plans using CPM/PERT graphs. IEEE Trans Power Syst 2007;22(3):1322–9.

[14] Duffey RB. Power restoration prediction following extreme events and disasters. Int J Disaster Risk Sci 2019;10(1):134–48.

[15] Čepin M. Probability of restoring power to the transmission power system and the time to restore power. Reliab Eng Syst Saf 2020;193:106595.

[16] Beyza J, Yusta JM. Integrated risk assessment for robustness evaluation and resilience optimisation of power systems after cascading failures. Energies 2021;14(7):2028.

[17] Liu Y, Fan R, Terzija V. Power system restoration: a literature review from 2006 to 2016. J Modern Power Syst Clean Energy 2016;4(3):332–41.

[18] Chakrabarty M, Sarkar D, Basak R. A comprehensive literature review report on basic issues of power system restoration planning. J Inst Eng (India) Ser B 2020;101(3):287–97.

[19] Haggi H, Song M, Sun W. A review of smart grid restoration to enhance cyber-physical system resilience. In: Proceedings of the 2019 IEEE innovative smart grid technologies-Asia (ISGT Asia); 2019. p. 4008–13.

[20] Fan D, et al. Restoration of smart grids: current status, challenges, and opportunities. Renew Sustain Energy Rev 2021;143:110909.

[21] Adibi M, Fink L. Power system restoration planning. IEEE Trans Power Syst 1994;9(1):22–8.

[22] Fink LH, Liou KL, Liu CC. From generic restoration actions to specific restoration strategies. IEEE Trans Power Syst 1995;10(2):745–52.

[23] Bosch J, Aniceto JM, Brunner KP. Ultrafast restoration after nationwide blackout: concept, principles & example of application. In: Proceedings of the 2020 international conference on smart energy systems and technologies (SEST); 2020.

[24] Edström F, Söder L. On uncontrolled system separation in power system restoration. In: Proceedings of the 2011 North American power symposium. IEEE; 2011.

[25] Edström F. On risks in power system restoration. KTH Royal Institute of Technology; 2011.

[26] Guttromson RT, et al. Human factors for situation assessment in grid operations. Richland, WA (United States): Pacific Northwest National Lab.(PNNL); 2007.

[27] Bell J, Holroyd J. RR679, review of human reliability assessment methods. Buxton: Health and Safety Laboratory for the Health and Safety Executive; 2009.

[28] Zhao Y, Smidts C. CMS-BN: a cognitive modeling and simulation environment for human performance assessment, part 1—methodology. Reliab Eng Syst Saf 2021;213:107776.

[29] Li R, Blanc KL. Approaches to human performance modeling of electric grids operators. In: Proceedings of the international conference on applied human factors and ergonomics. Springer; 2020.

[30] Li R, McJunkin TR, Blanc KL. Integrating operator function in work domain analysis of electric grid operations. In: Proceedings of the human factors and ergonomics society annual meeting. SAGE Publications Sage CA; 2020.

[31] Shuvro RA, et al. Correlating grid-operators' performance with cascading failures in smart-grids. In: Proceedings of the 2019 IEEE PES innovative smart grid technologies Europe (ISGT-Europe). IEEE; 2019.

[32] Shuvro RA, et al. Modeling cascading-failures in power grids including communication and human operator impacts. In: Proceedings of the 2017 IEEE green energy and smart systems conference (IGESSC). IEEE; 2017.

[33] Wang Z, et al. Impacts of operators' behavior on reliability of power grids during cascading failures. IEEE Trans Power Syst 2018;33(6):6013–24.

[34] Zhou Y, et al. Evaluation of human error probabilities of power grid dispatchers based on hybrid risk analysis method. In: Proceedings of the 4th international seminar on computer technology, mechanical and electrical engineering. IOP Publishing; 2020.

[35] Hao J, Qun Y. Simulation analysis of blackout model considering human factors. In: Proceedings of the 2021 2nd international conference on artificial intelligence and information systems. Association for Computing Machinery; 2021. p. 219.

[36] Hannaman G, Spurgin A, Lukic Y. A model for assessing human cognitive reliability in PRA studies. In: Proceedings of the conference record for 1985 IEEE third conference on human factors and nuclear safety; 1985.

[37] Magoua JJ, et al. Incorporating the human factor in modeling the operational resilience of interdependent infrastructure systems. Autom Constr 2023;149:104789.

[38] ENTSO-E System Operations Committee (SOC), Annex 5: policy on emergency and restoration, ENTSO-E. 2019.

[39] Cho J, et al. Exhaustive simulation approach for severe accident risk in nuclear power plants: OPR-1000 full-power internal events. Reliab Eng Syst Saf 2022;225:108580.

[40] Bolton ML, Zheng X, Kang E. A formal method for including the probability of erroneous human task behavior in system analyses. Reliab Eng Syst Saf 2021;213:107764.

[41] Shin SM, et al. STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system interactions. Reliab Eng Syst Saf 2021;213:107698.

[42] Hu Y, Parhizkar T, Mosleh A. Guided simulation for dynamic probabilistic risk assessment of complex systems: concept, method, and application. Reliab Eng Syst Saf 2022;217:108047.
[43] Swissgrid Transmission Code 2019, Swissgrid, 2020, Verband Schweizerischer Elektrizitätsunternehmen. https://www.swissgrid.ch/dam/swissgrid/customers/topics/transmission-code-2019-en.pdf.
[44] Bundesnetzagentur, Modalitäten für anbieter von systemdienstleistungen zum netzwiederaufbau, h.a.T.T. BW, . 2020, Bundesnetzagentur: https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2018/BK6-18-249/BK6-18-249_Vorschlag_vom_28_04_2020.pdf?__blob=publicationFile&v=2.
[45] Establishing a network code on requirements for grid connection of generators. C/2016/2001, COMMISSION REGULATION (EU); 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2016_112_R_0001.
[46] Establishing a guideline on electricity transmission system operation. C/2017/5310, Commission Regulation (EU); 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1485.
[47] Establishing a network code on electricity emergency and restoration. C/2017/7775, Commission Regulation (EU); 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2196.
[48] ENTSO-E System Operations Committee (SOC), Annex 1: policy on load-frequency control and reserves, ENTSO-E, . 2019.
[49] ENTSO-E System Operations Committee (SOC). Annex 2: policy on scheduling . 2019.
[50] Anderson M. Revitalising procedures. Health and safety executive. https://www.hse.gov.uk/humanfactors/topics/procinfo.pdf.
[51] UCTE O.H., Appendix 3: operational security, UCTE 2009: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_3_Appendix_final.pdf.
[52] Gooris M, et al. The use of eye tracking as a measure of situation awareness in power system control rooms. In: Proceedings of the 2022 IEEE Texas Power and Energy Conference (TPEC). IEEE; 2022.
[53] Leva MC. Transmission control centres and human interface design: the need to support situational awareness in the face of increasing complexity. In: Proceedings of the H-Workload2018: 2nd international symposium on human mental workload: models and applications; 2018.
[54] Giannuzzi, G., Pisani C., and Sattinger W., Generator coherency analysis in ENTSO-E continental system: current status and ongoing developments in Italian and Swiss case. IFAC-PapersOnLine, 2016. 49(27): p. 400–6.
[55] Reason J. Human error. Cambridge University press; 1990.
[56] Kulkarni V, Reddy S. Separation of concerns in model-driven development. IEEE Softw 2003;20(5):64–9.
[57] Kirwan B. A guide to practical human reliability assessment. CRC Press; 2017.
[58] Gertman D, et al. The SPAR-H human reliability analysis method. US Nuclear Regulatory Commission 2005. https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/cr6883.pdf.
[59] Ntuen C, Fang J. A simulation model of the adaptive human operator. In: Proceedings of the first industry/academy symposium on research for future supersonic & hypersonic vehicles. TSI Press; 1994.
[60] Simulink. [R2021a] 2021 2021; Available from: https://www.mathworks.com/products/simulink.html.
[61] Stateflow. [R2021a] 2021 2021; Available from: https://www.mathworks.com/products/stateflow.html.
[62] SimEvents. [R2021a] 2021 2021; Available from: https://www.mathworks.com/products/simevents.html.
[63] Simscape Electrical. [R2021a] 2021 2021; Available from: https://www.mathworks.com/products/simscape-electrical.html.
[64] Fogel LJ, Moore RA. Modeling the human operator with finite-state machines. NASA; 1968.
[65] Dang VN. Modeling operator cognition for accident sequence analysis: development of an operator-plant simulation. Nuclear engineering. Massachusetts Institute of Technology; 1996.
[66] Abreu JM, et al. Modeling human reliability in the power grid environment: an application of the spar-h methodology. In: Proceedings of the human factors and ergonomics society annual meeting. SAGE Publications Sage CA; 2015.
[67] Coyne KA. A predictive model of nuclear power plant crew decision-making and performance in a dynamic simulation environment. College Park: University of Maryland; 2009.
[68] Berry GL. The Weibull distribution as a human performance descriptor. IEEE Trans Syst Man Cybern 1981;11(7):501–4.
[69] McNeil AJ, Frey R, Embrechts P. Quantitative risk management: concepts, techniques and tools-revised edition. Princeton university press; 2015.
[70] Daneshkhah A, Oakley J. Eliciting multivariate probability distributions. Rethink Risk Meas Report 2010;1:23.
[71] Garthwaite PH, Kadane JB, O'Hagan A. Statistical methods for eliciting probability distributions. J Am Stat Assoc 2005;100(470):680–701.
[72] Mkrtchyan L, Podofillini L, Dang VN. Bayesian belief networks for human reliability analysis: a review of applications and gaps. Reliab Eng Syst Saf 2015;139:1–16.
[73] Pearl J. Fusion, propagation, and structuring in belief networks. Artif Intell 1986;29(3):241–88.
[74] Friend F. Cold load pickup issues. In: Proceedings of the 2009 62nd annual conference for protective relay engineers. College Station, Texas, USA: IEEE; 2009.
[75] Bianchetti L, et al. Inselnetzversuche im Übertragungsnetz. Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse. AES 2014;9(105):36–8.
[76] Nichelle'Le KC, Dobson I, Wang Z. Extracting resilience metrics from distribution utility data using outage and restore process statistics. IEEE Trans Power Syst 2021;36(6):5814–23.