The Change of Power System Response after Successive Faults

Jarno Lamponen  
Aalto University  
Helsinki, Finland  
jarno.lamponen@aalto.fi

Liisa Haarla  
Aalto University  
Helsinki, Finland

Emil Hillberg  
NTNU  
Trondheim, Norway  
emil.hilberg@ntnu.no

Ritva Hirvonen  
Fingrid Oyj  
Helsinki, Finland

Abstract—This paper illustrates the usefulness of visualizing the secure operating domains and the value of dynamic analyses when considering the vulnerability of a power system. The paper includes studies of the secure power transfer limits and vulnerabilities of the IEEE Reliability Test System (RTS). The limits and vulnerabilities are determined by simulating the dynamic response of single and multiple faults. The results are presented by visualizing the secure transfer domains as a function of the power flow on critical transfer corridors. The paper also provides an estimate for the frequency of blackouts related to the different operating domains. The results show how the vulnerability of the power system increases in steps as the amount of power transfer over a corridor increases.

Keywords—Vulnerability, security, stability, multiple contingencies

I. INTRODUCTION

Ensuring secure operation of a power system by identifying and mitigating vulnerabilities has been the topic for many rigorous studies. Several studies concentrate on a specific phenomenon that may jeopardize the security, such as cascading failures [1]–[4] or protective device failures [5]–[8]. Focusing on a specific phenomenon reveals vulnerabilities connected to the studied phenomenon but does not necessarily discover or value the vulnerabilities of other phenomena. Visualizing techniques such as nomograms have been used to describe $N-1$ security of a system [9], [10]. $N-1$ nomograms can give essential information to the system operator on the operating boundaries of normal operation. In general, multiple contingencies are not considered, thus failing to reveal the vulnerabilities beyond the normal operation conditions.

In [15] and [16], blackout phenomenon are described as a process with separate phases. In [15], these phases are suggested to be separated by distinctive transitions and are defined as: a thermally governed phase and an unstable phase. The work in [15] underlines the importance of analyzing multiple contingencies when assessing a power systems vulnerability to large disturbances. This paper continues the work presented in [15], where large European blackouts are analyzed and the importance of assessing the vulnerabilities related to dynamic instability is highlighted.

This paper presents a systematic analysis of the IEEE Three Area Reliability Test System 1996 (RTS) and quantifies vulnerabilities related to dynamic instability. The paper identifies the secure operating domains and critical vulnerabilities of the RTS by simulating the dynamical response of the system to faults. Phenomena defining the secure power transfer are described for different operating scenarios.

Two-dimensional nomograms of multilevel contingencies are used together with deterministic and probabilistic quantifications in order to illustrate the difference in vulnerability for various operational scenarios. Further development of the use of nomograms is presented in this paper, where vulnerability domains are identified based on the calculation of the system collapse frequency.

The paper is organized as follows: A short presentation of the RTS is included in Part II. Part III presents and visualizes the secure operating domains of the RTS. Part IV describes the vulnerability of the RTS deterministically and probabilistically. Part V describes the possibilities of mitigating blackouts. Part VI includes the discussion and conclusions.

II. IEEE RELIABILITY TEST SYSTEM 1996 (RTS)

To obtain a more realistic dynamic response of the RTS model than the original described in [11], detailed dynamic models are used to represent the synchronous generators, turbine-governors, and excitation system, as proposed by [12]. Further improvements on the RTS dynamic response have been made after the studies presented in this paper. These improvements may be found in [17], and are focusing on the voltage stability impact from load response and excitation system limiters.

A single-line diagram of the RTS is presented in Fig. 1. The optional HVDC connection as well as the control of the phase-shifting transformer, both connected between areas A and C, have been neglected in this study. Using HVDC or a phase-
shifter control could significantly improve the reliability of the system, as the power flows in the system could be better controlled in case of disturbances.

In several previous studies, the RTS has been used for analyzing the reliability limited to the (post-fault) adequacy rather than dynamic security of the power system. In this study, the added dynamic models have enabled the analysis of dynamic phenomena related to faults, i.e., the security. The dynamic analyses reveal the vulnerabilities that have remained hidden in the studies based merely on steady state power flow analyses.

III. THE SECURE OPERATING DOMAIN

The first part of this section describes a dynamic $N-1$ contingency analysis of the RTS, with a secure operating domain identified and visualized from these results. The second part describes the $N-k$ security of the RTS, and visualizes an $N-2$ secure operating domain of the system. These studies are based on analyses on approximately 50 different operating scenarios. It should be noted that an infinite number of operating scenarios are possible, thus this study only covers a part of the total operational space and can only identify the vulnerabilities of the studied scenarios.

A. $N-1$ security assessment

A dynamic $N-1$ contingency analysis with generator trips and line faults was performed on the RTS. The studied line faults were three-phase faults with 100 ms duration, followed by a permanent trip of the faulted line. Line fault locations were near the line ends. The total number of studied contingencies was approximately 300. The list of contingencies together with the selected operating scenarios results in an $N-1$ contingency analysis based on around 15000 dynamic simulations. Based on this $N-1$ contingency analysis, the stability of the transition from the pre-fault state to the post-fault state, as well as the adequacy (line loading and voltage levels) of the post-fault steady state were assessed.

The angle differences over the line connecting area B and area C for all single line faults (with subsequent line tripping) of operating scenario X (see Table I and Fig. 3). Blue curves correspond to faults resulting in stable operation, while the fault and trip of the line connecting area A and area C result in an unstable system (red curves).

![Fig. 2. Angle difference over the line connecting areas B and C for all single line faults (with subsequent line tripping) of operating scenario X (see Table I and Fig. 3). Blue curves correspond to faults resulting in stable operation, while the fault and trip of the line connecting area A and area C result in an unstable system (red curves).](image)

### Fig. 1. Single-line diagram describing the IEEE Reliability Test System 1996 [11]. The dimensions do not reflect the line lengths.
cases were identified among the studied scenarios. Inside this circle, no transient instability dynamic studies of line faults and generator trips in different limitations induced by transient stability and defined by the limits for the lines. The circle in Fig. 3 represents the term emergency ratings defined in [11] were used as thermal operating domain are presented as a rectangle in Fig. 3. Long other dimension is the power flow on the corridor between areas A and B. These transfer corridors directly from the system topology due to the weak connections between the three meshed areas. These transfer corridors can be used to visualize the secure operating domains of the system. In case of a multi-corridor system, such as the RTS, this would imply a multi-dimensional space. However, here we use more comprehensible two-dimensional illustrations for visualizing the secure operating domains. In this paper, two corridors connecting area C to the other areas are combined to form one dimension ‘area C surplus’ while the other dimension is the power flow on the corridor between areas A and B.

By using the two-dimensional space of ‘power flow A–B’ and ‘area C surplus’, the thermal limitations of the secure operating domain are presented as a rectangle in Fig. 3. Long term emergency ratings defined in [11] were used as thermal limits for the lines. The circle in Fig. 3 represents the limitations induced by transient stability and defined by the dynamic studies of line faults and generator trips in different power flow cases. Inside this circle, no transient instability cases were identified among the studied scenarios.

### Table I

<table>
<thead>
<tr>
<th>Inter-area power exchange of studied operating scenarios X and Y.</th>
<th>Case X</th>
<th>Case Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power flow from area A to B (MW)</td>
<td>220</td>
<td>255</td>
</tr>
<tr>
<td>Power flow from area A to C (MW)</td>
<td>-240</td>
<td>-150</td>
</tr>
<tr>
<td>Power flow from area B to C (MW)</td>
<td>420</td>
<td>365</td>
</tr>
<tr>
<td>Area A Power export (MW)</td>
<td>15</td>
<td>-105</td>
</tr>
<tr>
<td>Area B Power export (MW)</td>
<td>-640</td>
<td>-620</td>
</tr>
<tr>
<td>Area C Power export (MW)</td>
<td>655</td>
<td>515</td>
</tr>
</tbody>
</table>

**B. The $N−1$ security operating domain**

For the RTS, it is possible to identify critical transfer corridors directly from the system topology due to the weak connections between the three meshed areas. These transfer corridors can be used to visualize the secure operating domains of the system. In case of a multi-corridor system, such as the RTS, this would imply a multi-dimensional space. However, here we use more comprehensible two-dimensional illustrations for visualizing the secure operating domains. In this paper, two corridors connecting area C to the other areas are combined to form one dimension ‘area C surplus’ while the other dimension is the power flow on the corridor between areas A and B.

In Fig. 3, operating scenarios may be identified where a single fault leads to unstable operation even though the thermal limits are not exceeded in the post fault state (i.e. the domain inside the rectangle but outside the circle). Thus, $N−1$ secure operating domain for the RTS would not have been defined correctly without the stability assessments.

**C. The $N−k$ secure operating domain**

The most critical contingencies identified in the $N−1$ contingency analysis are the faults and trips of lines in the transfer corridors between areas A, B, and C. These contingencies were selected as the first contingency in an $N−2$ contingency analysis. Thus, the $N−2$ contingency analysis comprise of approximately 15000 dynamic simulations.

Fig. 4 presents the $N−2$ secure transmission limits for two successive line faults. A line disconnection significantly reduces the thermal limits between areas A and B compared with the $N−1$ limits of the intact grid. The reason for this is that there are two 230 kV lines and one 138 kV connecting areas A and B. If one 230 kV line is disconnected, there is still one 230 kV line and one 138 kV line, and the thermal $N−1$ limit between the area A and B is roughly equal to the power that these lines can carry together (the alternative long path via area C does not carry significant amount of power). However, if two 230 kV lines are disconnected, there is only one 138 kV line between the areas in addition to the longer transfer path via area C. Now a relatively larger share of the power will flow via area C in the $N−2$ case compared with the $N−1$ case. The overall impact of this path on the transfer capacity between areas A and B is small due to the high impedance. Therefore, the difference between the thermal $N−1$ limit, shown in Fig. 3, and the $N−2$ limit, shown in Fig. 4, is roughly the thermal capacity of one 230 kV line connecting areas A and B.
The disconnection of any single line in the transfer corridors between areas A, B, and C has a smaller effect on transient angle stability limits than on thermal limits because the disconnection of any of these lines does not significantly affect the operating state of the generators (if the operating scenario is within the secure operating domain). However, line disconnections weaken the ability of the grid to absorb the kinetic energy from the generators, which explains the reduction from the transient angle $N-1$ limit to the $N-2$ limit.

When considering stable power transfers between areas A and B, the most critical combination of the successive $N=2$ line faults was the trip of both 230 kV lines connecting areas A and B. The same $N=2$ fault combination also dominates the reduction in the thermal limits.

The main difference between the thermal and stability limitations are that the thermal limits do not depend on the order of occurrence of the faults, whereas for stability, the order of the fault sequence and also the time between the faults are significant. The consequences can be completely different depending if the transient from the previous fault has stabilized or not when a second fault occurs. In this study, the system was assumed to have reached a steady state between subsequent faults. The most critical order of the faults was the following: first a fault and trip of ARNE–BARTON line (a 230 kV line from area A to area B) followed by a line fault near bus AUSTEN in area A and the trip of the other 230 kV line between area A and area B; AUSTEN–BATES line.

When considering the power surplus and deficit of area C, the most restricting set of successive $N=2$ line contingencies is the disconnection of both lines connecting area C to other areas. This will isolate area C, and successful islanding requires that the available reserve power cover the power deficit in each isolated area. Furthermore, island operation also requires suitable power and frequency controls.

Assuming that the frequency controlled instantly activated reserves equal 400 MW (the largest unit in the system) divided evenly between the areas (in each area the largest unit has the same size), results in 133 MW reserves in each area. Thus, the power deficit of area C in the initial operating scenario cannot exceed 133 MW to ensure successful islanding. Similarly, the power surplus of area C cannot exceed 266 MW to ensure that areas A and B have the required reserve power. In Fig. 4, the dotted lines represent these frequency stability limits. The rectangular thermal $N-1$ and $N-2$ limits, illustrated in Fig. 3 and Fig. 4 respectively, are equal in 'C surplus' dimension because if both lines connecting area C to other areas are tripped, there remain no lines that could be overloaded.

**D. Change in system response**

If the operating scenario is not within a secure operating domain, and a fault occurs, the consequences are significantly different if the thermal limits of the lines are exceeded or the stability of the system is jeopardized.

As described in the previous sections, when determining the secure power transfer limits, the limit is the one that is the lowest: either the thermal current carrying capacity of the lines after a fault, the ability of the generators to maintain the synchronism, or stable voltages during and after a fault transient.

In the case with thermal limitations, overloading may eventually lead to protective actions that disconnect the overloaded component. Depending on the protection scheme and the level of overload, the protection may act in a few seconds or after several minutes. This protective action may lead to an increased loading of parallel components, leading to further protective actions in a (often rather slow) cascade. This part of a blackout process may be referred to a thermally governed phase [15]. If the cascade continues, at some stage it will lead to instability.

If stability limitations are exceeded, the system enters an unstable and uncontrollable state, referred to as the unstable phase of the blackout process [15]. This phase is characterized by one or several of the following dynamic phenomena: oscillations of voltage, power, or frequency, or the decay (or rise) in voltage or frequency. Such phenomena often lead to the triggering of several component protections, where the affected area of the power system is difficult to anticipate.

The consequences after exceeding stability limitations are usually faster and more wide-spread and therefore more severe than the consequences of exceeding thermal limits. Therefore, it is crucial to know not only of the actual security limits of the system, but the response of the system and the phenomenon that is limiting the system at different operating scenarios. For a system, originally limited by the thermal capacity of the lines, the loss of stability after it has faced several contingencies, corresponds to a change of the system response.
The vulnerability of a given operating scenario can be assessed deterministically by studying the combinations of contingencies that cause system-wide consequences. The vulnerability of the system can thus be assessed using the indicator, $k_{\text{min}}$, defined in [15] as:

$$k_{\text{min}} = \min (s_1, s_2, \ldots, s_n),$$

where $s_i$ is a set of contingencies leading to an unstable state at the specific operating scenario. The indicator describes the minimal number of contingencies after which instability occurs. Fig. 6 illustrates the vulnerability level quantified by the $k_{\text{min}}$ indicator for the RTS, where $k_{\text{min}} \geq 3$ indicates that the stability of the system is not threatened by any of the studied double contingencies.

In the studied $N-1$ and $N-2$ contingencies, the fault sequences leading to system collapse consist of faults on the lines on the transfer corridors between areas A, B, and C as well as generator trips.

B. System collapse frequency as probabilistic indication of vulnerability

The frequency of a system collapse can be assessed by identifying the specific chains of events leading to the collapse. For a given operating scenario $o_i$, the frequency of a system collapse $F^{o_i}$ that takes into account $N-1$, $N-2$ and $N-3$ contingency sets can be calculated as follows:

$$F^{o_i} = \sum_{N-1} f_{1}^{o_i} + \sum_{N-2} f_{m}^{o_i} P_{n}^{o_i} + \sum_{N-3} f_{r}^{o_i} P_{s}^{o_i} P_{t}^{o_i},$$

where $f_{i,m,n,r}$ is the frequency of the occurrence of a fault in contingency set $N-k$, $P_{s,m,n}$ is the conditional probability that an additional fault occurs before mitigating actions have been performed. The term with a minimum number of faults that lead to a collapse dominates in (2) and thus gives an estimation of the system collapse frequency. Therefore, the $N-2$ and other higher-order events, which consist of a two or more successive independent contingencies, have less effect on the system collapse frequency than the lower order events.

For the RTS, different domains of vulnerability caused by consecutive line faults are presented in Fig. 7. An estimation of the system collapse frequency is determined for every vulnerability domain (1–8 in Fig. 7) by summing the frequencies of the critical events. The critical events are chains of events that may consist of faults that cause instantaneous instability but also faults that lead to instability by causing overloading and a fault of another line. Table II presents the estimated system collapse frequencies.

When estimating the system collapse frequency, it is assumed that mitigating actions to reduce power transfer in time, in case of line overloads, fail with the probability of 1%, which causes a new line fault. The outage data of [11] is used for estimating the frequency of $N-2$ contingencies.

The first fault has the frequency of 'permanent outage' in [11] and the frequency of the second fault is the sum of permanent and transient outages in [11]. In the dynamic simulations, all the line faults were three-phase faults.
The system collapse frequency as a function of power surplus in area C when power transfer from area A to area B is 0 MW is presented in Fig. 8. Thus, the system collapse frequency illustrated in Fig. 8 corresponds to a move along the Y-axis in Fig. 7 from the \( N^{-1} \) secure domain to the unsecure domain. In Fig. 8, the vulnerability increases in steps when the power flow exceeds certain limits. The steps are caused by the drastic increase in the number of single and multiple faults leading to undesired system consequences, which occur when the power flow exceeds the identified limits. The steps correspond to the border lines between the vulnerability domains in Fig. 7.

The faults and fault combinations occur with a certain probability on a given time period and are independent of the power flow. The increment of the system collapse frequency is especially significant when the power flow exceeds the \( N^{-1} \) secure level.

C. Impact of protection system and circuit breaker failures

Failures of protection systems have been identified to have significant impact on events leading to a system collapse [6]. Protective device misoperations may aggravate the consequences of disturbances by leading to further disconnections or even transform the system directly to an unstable operating state. The failure of the circuit breakers or main protective relays to separate the faulty component of the system leads to further disconnections by the back-up protection or by the breaker failure relay. More importantly, it always extends the fault duration, which may lead to generators falling out-of-step and thus initiate a process leading to system collapse.

Fig. 8. The estimation of the RTS system collapse frequency [1/year] as a function of the area C power surplus. The power transfer from area A to B is 0 MW. The dotted line represents the \( N^{-1} \) secure transfer limit.

The system collapse frequency as a function of power surplus in area C when power transfer from area A to area B is 0 MW is presented in Fig. 8. Thus, the system collapse frequency illustrated in Fig. 8 corresponds to a move along the Y-axis in Fig. 7 from the \( N^{-1} \) secure domain to the unsecure domain. In Fig. 8, the vulnerability increases in steps when the power flow exceeds certain limits. The steps are caused by the

**Table II**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Restricting fault (set) and phenomenon</th>
<th>Estimation of system collapse frequency [1/year]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( 113 \rightarrow 215 ) or ( 123 \rightarrow 217 ) or ( 121 \rightarrow 325 ) or ( 223 \rightarrow 318 )</td>
<td>&gt;1</td>
</tr>
<tr>
<td>2</td>
<td>( 121 \rightarrow 325 ) and ( 223 \rightarrow 318 )</td>
<td>1.38E-2</td>
</tr>
<tr>
<td>3</td>
<td>( 113 \rightarrow 215 ) and ( 123 \rightarrow 217 ) or ( 121 \rightarrow 325 ) and ( 223 \rightarrow 318 )</td>
<td>5.03E-3</td>
</tr>
<tr>
<td>4</td>
<td>( 121 \rightarrow 325 ) and ( 223 \rightarrow 318 )</td>
<td>2.99E-3</td>
</tr>
<tr>
<td>5</td>
<td>( 121 \rightarrow 325 ) and ( 223 \rightarrow 318 )</td>
<td>2.97E-3</td>
</tr>
<tr>
<td>6</td>
<td>( 113 \rightarrow 215 ) and ( 123 \rightarrow 217 )</td>
<td>2.06E-5</td>
</tr>
<tr>
<td>7</td>
<td>( 113 \rightarrow 215 ) and ( 123 \rightarrow 217 )</td>
<td>2.06E-5</td>
</tr>
<tr>
<td>8</td>
<td>&lt;2.06E-5</td>
<td></td>
</tr>
</tbody>
</table>
actions might be required within fractions of a second after the blackout. To prevent transient instability, the response of such not in a secure state, mitigating actions can be used to prevent a generation. If a critical contingency occurs when the system is phase-shifting transformers, or re-dispatching of power flows of AC lines by controlling HVDC links, using TSO can use several preventive actions such as change the ensure that the system remains at a secure operating point, the spread consequences caused by critical contingencies. To analyze this response to identify the vulnerabilities related to protection system and circuit breaker failures.

Since a stuck circuit breaker during a line fault should also be regarded as an $N-2$ fault, additional simulations have been performed to analyse the system impact of such failures. Here, bus fault simulations were made for every bus in the RTS. The fault duration was selected to 250 ms, reflecting a fault sequence with a line fault, having a stuck circuit breaker at one line end and the clearing of the fault by the breaker failure protection. Simulations were done for all previously studied operational scenarios, resulting in an additional 3500 dynamic simulations. In contrast to the successive line faults, which resulted in instability for some operating scenarios, a 250 ms fault at buses located near large generators resulted in transient instability of all the studied operating scenarios. Therefore, for the RTS, a stuck circuit breaker during a line fault can be regarded as the most critical $N-2$ fault.

V. MITIGATION OF LARGE DISTURBANCES

It is possible to implement remedial actions to prevent wide spread consequences caused by critical contingencies. To ensure that the system remains at a secure operating point, the TSO can use several preventive actions such as change the power flows of AC lines by controlling HVDC links, using phase-shifting transformers, or re-dispatching of power generation. If a critical contingency occurs when the system is not in a secure state, mitigating actions can be used to prevent a blackout. To prevent transient instability, the response of such actions might be required within fractions of a second after the undesired event has occurred; hence, only automatic actions are possible to prevent instability.

One solution to mitigate blackouts is the implementation of system integrity protection schemes (SIPS), which are, in contrast to common component protection, designed to preserve the power system integrity during abnormal conditions. A possible classification of SIPS is on the type of predefined events, such as breaker tripping signals) or response-based (measuring electrical parameters, e.g. frequency or voltage).

Three SIPS solutions have been studied with the RTS, utilizing different activation signals:
- SIPS$_{CB}$: activated by status signals from circuit breakers
- SIPS$_{V}$: activated by voltage angle measurements
- SIPS$_{f}$: activated by frequency measurements

The results for the critical contingency of operating scenario X, shown in Fig. 9, illustrate the possibilities to prevent the system from becoming unstable. Here, an internal arming of the response-based SIPS is used together with a time delay to prevent unwanted action during switching events. Based on a dynamic contingency analysis described in [13], arming and activation signal magnitudes have been selected as:

- $\Delta\delta_{BC}$ - arming: $40^\circ$ for 200ms, activation: $50^\circ$.
- $\Delta\delta_{AC}$ - arming: $0.2$Hz for 200ms, activation: $0.25$Hz.

The total delay between measurement and the implementation of mitigating action is assumed to be no longer than 100 ms.

Depending on the fault location, the transient behavior of the system sets different requirements on the response time of the SIPS solution. Such is also the case with different fault types and fault durations, meaning that the SIPS may not prevent instability in all scenarios.

The response-based solutions, SIPS$_{V}$ and SIPS$_{f}$, are not as fast as the event-based, SIPS$_{CB}$. The event-base SIPS will efficiently and fast provide the actions foreseen as sufficient to prevent the transient instability. However, since the trigger signal of the SIPS$_{CB}$ is based on the triggering of specific protections, the system is not protected against unforeseen events. The response-based SIPS will be able to provide increased protection against multiple or unforeseen contingencies, but might need longer response time depending on how the SIPS are designed.

VI. DISCUSSION AND CONCLUSIONS

When performing a comprehensive vulnerability analysis, also post fault dynamics should be included. Studies based on steady state analyses can erroneously indicate “secure” operation outside the $N-1$ stable domain, as the domain outside the circle but inside the rectangle in Fig. 3 clearly illustrates. It should also be noted that, when stability is an issue, an outage is not the only concept that should be analyzed since it is the fault that accelerates the generators.

Furthermore, a line trip may weaken the system and lead to cascading disconnections due to instability. Thus, studies
where dynamics are ignored may provide too optimistic results since they do not reveal vulnerabilities connected to instability. In our case study, the instability occurred inside the steady state (thermal) limits, a result that cannot be reached with steady state analyses only. In some cases, it may be possible to provide angle stability limits using simplified models as [14] shows.

A proper identification of power system vulnerabilities requires knowledge of the dynamic behavior of the system in disturbed conditions and awareness of a possible change in the system response after several faults. Therefore, dynamic $N = 2$ or even higher-order contingency analyses should be used in power system vulnerability assessments. As the vulnerabilities are identified, mitigating actions can be planned and implemented.

It is shown in this paper that the vulnerability of the power system may increase in distinct steps as the amount of power transfer is increased over the critical corridors. Thus, increasing power transfer above certain limits may drastically increase the number of faults or fault combinations with undesired consequences.

For the system operator, the identification of the secure operating conditions is essential, and nomograms may support identification of vulnerabilities of the system at different operating conditions. Nomograms can provide information of the existing restrictions on the secure transfer capacity as well as the margin to the security limits in an illustrative manner. In this paper two-dimensional illustrations are favored over multidimensional when visualizing the secure operating domain, this is done since two-dimensional illustrations are usually more comprehensible to the observer. The illustrations in this paper are based on the power transfer over critical corridors of the RTS system. For other systems, it may be more feasible to select other parameters, e.g. the demand in certain areas, as limiting factors. The presented visualizations of operating domains for the RTS are symmetrical in relation to power transfer, due to the symmetrical topology of the RTS.

If the circuit breakers or main protective relays fail to disconnect the faulted component from the grid, the fault duration extends and several components are tripped by the breaker failure relays or by the back-up protection. This type of faults should be considered as multiple contingencies and must be included when assessing the risk of system collapse. Simulations made on the RTS system underlines the importance of considering this type of faults since the extended fault duration near critical generators significantly increases the risk of large disturbances, even in operating scenarios with a lightly loaded grid.

Simulation results presented in this paper highlight the value of dynamic analyses, and illustrate that analyses based on steady-state studies (load flow) may overestimate the security of the system as they cannot reveal the vulnerabilities related to the dynamic response of the system. Therefore, dynamic analyses should be considered imperative in security and vulnerability assessment studies.

REFERENCES


