A Trend-Oriented Power System Security Analysis Method Based on Load Profile

Anjia Mao and M. Reza Iravani, *Fellow, IEEE*

***Abstract*—Conventional power system security analysis based on multiple case studies cannot predict all operational states and hence neither guarantees an adequate security margin nor an economical operation for the power system. Based on the trend analysis method which is used in the field of economics, this paper introduces the concept and a methodology for "trend security analysis" of power systems. This method utilizes the load profile forecast and the contingency occurrence probability and determines the system security trend in the subsequent time window. Based on a recursive algorithm which is developed by utilizing the higher order derivatives of power flow equations, this paper also presents a method for fast determination of the trend variations of the system states and security indices. Three IEEE test systems are used to demonstrate the applications of the proposed concepts, evaluate their performance and verify their accuracy.**

***Index Terms*—Power system security, process-oriented method, security analysis, security trend analysis.**

I. Introduction

POWER system security analysis is a necessary means to ensure the secure operation of power systems. According to the mathematical model, security analysis can be classified into static analysis and dynamic analysis [1]. Dynamic security concerns, e.g., power system oscillatory modes, transient instability, frequency instability, are seldom caused by a single apparatus failure. Thus, security analysis is more focused on system behavior subsequent to a contingency [2]. This paper deals with static security analysis after a contingency.

Power flow equations are the basis for power system static security analysis. Since an analytical solution of power flow equations is not attainable [3], [4], power system security analysis is primarily based on multiple case studies. To assure a sufficient security margin, the most severe scenario is often used for security analysis. Generally the most severe scenario is based on maximum load-generation case and may suffer from one or more of the following.

- A single case study, even under maximum load-generation, cannot cover all operational scenarios, since the system states change with the load variations, and the load variations at various buses are not necessarily consistent.
- Most probably a single case study is far different from the actual system operating conditions and thus the analysis result corresponds to neither an economical nor a secure system operation.
- A single case study which can reveal the outcome of cascading failures due to multiple contingencies is unlikely since cascading failures are almost unpredictable.

To address such issues, online security assessment, $N-1-1$ contingency analysis, cascading failure simulation, and process oriented analysis have been proposed. For example [5] discusses an integrated platform and [6] designs a set of risk evaluation indices for power system security assessment. Reference [7] utilizes an $N-1-1$ analysis methodology in Midwest ISO's NERC-compliance studies. The method is composed of a 3-step process of "$N-1$ analysis, optimal power flow and $N-1$ analysis" which can demonstrate the actual operation of the system and hence is more flexible and practical [8]. References [9]–[11] use artificial intelligence methods to simulate the occurrence of a cascading failure and evaluate its impacts on the power system, and [12] presents a conceptual design of a multi-agent system for restoration of an interconnected power system after a cascading failure.

Different from traditional single-study-case-based method, the model of the trend security analysis in this paper is based on the load profile forecast. By utilizing higher order derivatives of power flow equations, the model is solved by the Taylor series expansion method. A recursive algorithm, which can efficiently determine the trend variations of the system states and security indices, is adopted. The model covers most of the operational scenarios since it is based on a rolling operational process. Because all cases in the process are quickly solved, no process partition and no characteristic case identification approach [13]–[15] is needed to improve the calculation speed.

The trend-oriented power system security analysis method, which determines the system security trend in the time window subsequent to the current time window, is not based on the most severe scenario and hence can result in a superior economical operation under the condition that adequate security margin is assured. The method can also reveal the outcome of cascading failures when it is implemented by an online and rolling operation mode. Therefore, the application of the trend security analysis method can provide the operator an effective means to grasp the security trend of the power system and ensure the system security and economic operation.

Manuscript received May 21, 2013; revised August 19, 2013 and October 16, 2013; accepted November 12, 2013. Date of publication November 25, 2013; date of current version April 16, 2014. This work was supported by the Fundamental Research Funds for the Central Universities. Paper no. TPWRS-00639-2013.

A. Mao is with the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China, and also with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: angel_maoyang@163.com).

M. R. Iravani is with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: iravani@ecf.utoronto.ca).

Digital Object Identifier 10.1109/TPWRS.2013.2291400

The rest of this paper is organized as follows. In Section II, the trend analysis theory and its applications in power system is reviewed, and then the security trend is defined and classified. Section III introduces a fast method for process security analysis. In Section IV, a security trend analysis model is developed. Section V provides the testing scenarios and simulation results. Section VI provides a discussion and states the conclusions of this paper.

II. Brief Review of Trend Analysis Theory and Its Applications in Power Systems

Fluctuation of the commodity prices presents a certain time varying pattern. The changes in the pattern constitute the price trend [16]. The trend theory displays the rules of the supply-demand balance, subject to the internal and external factors to identify the best trading opportunities in a market [17], [18].

Although the trend analysis theory is developed for the stock and commodity market, it has also been widely used in medical sciences, biology, geology, and even the military field. For example [19] introduces the process and experience of applying the trend techniques to support the US Navy F/A-18C series aircraft level integrated health monitoring system, which is a highly complicated system within a high pressure environment, with an extremely low tolerance for errors by improving the corrective and preventative maintenance cycles. In [20], a trend analysis method is used to evaluate the F-22 fleet subsystem wear out issues due to vibrations, thermal, humidity and corrosion factors, and as a result a reliability growth curve model is proposed.

In the fields of electrical engineering, some researchers have also probed into the applications of trend analysis theory, such as signal processing, load forecasting, fault prediction and detection, parameter identification, and stability analysis. For example [21] presents a linear least-square method to estimate the Fourier coefficients and trend components of a periodic time series. In [22], a weighted largest Lyapunov exponent forecasting method and the associate trend adjustment technique are used to forecast the long-term electricity demand. Similarly, [23] and [24] also use trend analysis method for medium or short-term electric energy demand forecasting. Reference [25] proposes a trend analysis technique for incipient fault prediction and [26] investigates a timed-event trend analysis method to evaluate and identify symptom parameters for incipient fault detection. Reference [27] provides a statistical approach to estimate the trend in variation of electrical parameters. Based on a trend analysis method, and [28] proposes a variable and a generalized rule induction model to detect the non-technical losses in power companies. Reference [29] proposes a statistical framework for analyzing and estimating time-varying trends in measured data. Reference [30] proposes a nonstationary time-frequency analysis method to identify nonlinear trends and filtering frequency components of a large system dynamics, and [31] presents an expert system for security trend analysis of a stability-limited power system. These attempts have resulted in a new concept and methodology for power system analysis and are worthy of further investigations.

The security of a power system depends on the system operating conditions and the contingent probability of disturbances. To determine the security level of a power system, not only a specific study case under certain contingency should be carried out, but also variations of the system state and different contingent probabilities must be taken into account. Therefore, power system security trend is defined as the future security performance index under certain contingent probability. The security trend of power system can be divided into the long-term trend, the medium-term trend, the short-term and the ultra-short-term trend. However, from the perspective of operation and control, the system dispatcher or operator is mainly concerned with the short term rather than the long term trends. Therefore, this paper focuses on the short-term trend within the time frame of a few hours.

The security trend analysis requires calculation of the security index of the system in the subsequent time period, and hence, it requires a fast process-oriented analysis method.

III. Fast Process-Oriented Security Analysis Method

Assume the load variation is slow and the transient process can be ignored. Hence the static equations can be used to describe the system state. Suppose the load profile of each bus has been obtained through a nodal load forecasting method. Thus the power flow of bus i can be expressed as

$$\hat{\dot{V}}_i(t)\sum_{j=1}^{N} Y_{ij}(t,c(t))\dot{V}_j(t) = \hat{S}_i(t) \tag{1}$$

where $V_i(t)$ is the voltage curve and $S_i(t)$ is the load profiles of bus i. $Y_{ij}(t,c(t))$, whose value depends on contingency $c(t)$, is the mutual admittance between bus i and j. $\hat{S}_i(t)$ and $\hat{\dot{V}}_i(t)$ are respectively the conjugation of $S_i(t)$ and $\dot{V}_i(t)$, where the dot notation means that the voltage is a phasor. Since the load curve $S_i(t)$ is composed of a series of discrete components $S_{i,k}, k = 1,2,\ldots,N$, (1) can be discretized as

$$\hat{\dot{V}}_{i,k}\sum_{j=1}^{N} Y_{ij,ck}\dot{V}_{j,k} = \hat{S}_{i,k}, \quad k = 1,2,\ldots,N \tag{2}$$

where N is the number of the discrete cases included in the interval. Equation (2) is a series of power flow equations and the problem is to efficiently solve these equations for fast calculation of the security indices. The following algorithm provides an efficient solution. First the Taylor series expansion of power flow equations is introduced.

A. Taylor Series Expansion of Power Flow Equations

In (1), suppose no contingency has occurred in the interval of $[t_0, t_M]$. Separating the real and imaginary parts and re-organizing in a matrix form

$$\begin{bmatrix} V_{ix}(t) & V_{iy}(t) \\ -V_{iy}(t) & V_{ix}(t) \end{bmatrix} \sum_{j=1}^{N} \begin{bmatrix} G_{ij} & -B_{ij} \\ B_{ij} & G_{ij} \end{bmatrix} \begin{bmatrix} V_{jx}(t) \\ V_{jy}(t) \end{bmatrix} = \begin{bmatrix} P_i(t) \\ -Q_i(t) \end{bmatrix} \tag{3}$$

where V_{ix} and V_{iy} are the real and imaginary parts of the node voltage V_i. Taking mth-order derivatives of both sides of (3) and applying the binomial theorem

$$\sum_{k=0}^{m} C_m^k \begin{bmatrix} V_{ix} & V_{iy} \\ -V_{iy} & V_{ix} \end{bmatrix}^{(m-k)} \times \left(\sum_{j=1}^{N} \begin{bmatrix} G_{ij} & -B_{ij} \\ B_{ij} & G_{ij} \end{bmatrix} \begin{bmatrix} V_{jx} \\ V_{jy} \end{bmatrix} \right)^{(k)} = \begin{bmatrix} P_i \\ -Q_i \end{bmatrix}^{(m)}. \quad (4)$$

Let

$$\sum_{j=1}^{N} \begin{bmatrix} G_{ij} & -B_{ij} \\ B_{ij} & G_{ij} \end{bmatrix} \begin{bmatrix} V_{jx} \\ V_{jy} \end{bmatrix} = \begin{bmatrix} A_i \\ B_i \end{bmatrix} \quad (5)$$

and

$$\sum_{j=1}^{N-1} \begin{bmatrix} G_{ij} & -B_{ij} \\ B_{ij} & G_{ij} \end{bmatrix} \left(\begin{bmatrix} V_{jx} \\ V_{jy} \end{bmatrix} \right)^{(k)} = \begin{bmatrix} A_{ik}^{(k)} \\ B_{ik}^{(k)} \end{bmatrix}. \quad (6)$$

Then (4) can be rewritten as

$$\begin{bmatrix} B_i & -A_i \\ A_i & B_i \end{bmatrix} \begin{bmatrix} V_{ix} \\ V_{iy} \end{bmatrix}^{(m)} + \begin{bmatrix} -V_{iy} & V_{ix} \\ V_{ix} & V_{iy} \end{bmatrix} \times \sum_{j=1}^{N} \begin{bmatrix} G_{ij} & -B_{ij} \\ B_{ij} & G_{ij} \end{bmatrix} \begin{bmatrix} V_{jx} \\ V_{jy} \end{bmatrix}^{(m)} = \begin{bmatrix} -Q_i \\ P_i \end{bmatrix}^{(m)} - \sum_{k=1}^{m-1} C_m^k \begin{bmatrix} V_{ix}^{(m-k)} B_{ik} - V_{iy}^{(m-k)} A_{ik} \\ V_{ix}^{(m-k)} A_{ik} + V_{iy}^{(m-k)} B_{ik} \end{bmatrix}. \quad (7)$$

For each bus, an equation similar to (7) can be obtained. If the bus is a PV bus, then the equation corresponding to Q is replaced by

$$[2V_{ix} \quad 2V_{iy}] \begin{bmatrix} V_{ix}^{(m)} \\ V_{iy}^{(m)} \end{bmatrix} = -\left(\sum_{k=1}^{m-1} C_m^k V_{ix}^{(m-k)} V_{ix}^{(k)} + \sum_{k=1}^{m-1} C_m^k V_{iy}^{(m-k)} V_{iy}^{(k)} \right). \quad (8)$$

Equations (7) and (8) show that if the initial V_{ix} and V_{iy} are known, then the coefficient matrix is constant and can be factorized to improve the efficiency. The right-hand side vector is recursive, i.e., to calculate the kth-order derivatives of V_{ix} and V_{iy}, the vector only depends on the $1st, 2nd, \ldots, k-1th$ order derivatives. Therefore, the algorithm is fast and straightforward to implement.

After all derivatives of V_{ix} and V_{iy} are obtained, the Taylor series or Maclaurin series can be used to deduce the real and imaginary parts of the node voltage V_i, if the Taylor series expansion converges, i.e.,

$$\begin{cases} V_{ix}(t) = V_{ix0} + \sum_{k=1}^{m} \frac{V_{ix}^{(k)}}{k!} (\Delta t)^k \\ V_{iy}(t) = V_{iy0} + \sum_{k=1}^{m} \frac{V_{iy}^{(k)}}{k!} (\Delta t)^k. \end{cases} \quad (9)$$

The validity of (9) can be verified with $V_{ix}^{(m)}$ and $V_{iy}^{(m)}$, i.e., if they are bounded, then the Taylor series converges. This condition is not difficult to satisfy, because under normal circumstances, the operating state of power system varies only in a limited range.

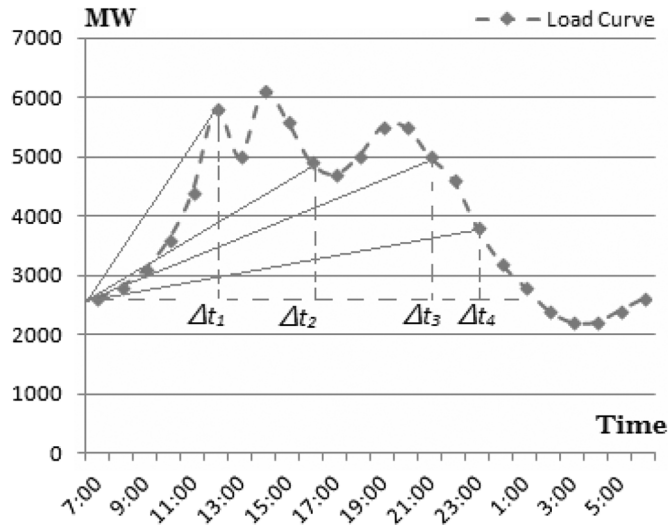

Fig. 1. Assumed pattern for daily load change.

As described before, the load profile is composed of a series of discrete cases and only these cases need to be solved. Therefore, there is no need to focus on the specific shape of the load variations and one can assume that the change from the initial point to the destination point is a straight line, as shown in Fig. 1.

Thus, if the load P_{i0}, Q_{i0} at the initial point is already known, then (10) can be used to obtain the higher-order derivatives of P and Q:

$$\begin{bmatrix} P_i \\ -Q_i \end{bmatrix}^m = \begin{cases} \begin{bmatrix} (P_{is} - P_{i0})/\Delta t \\ -(Q_{is} - Q_{i0})/\Delta t \end{bmatrix}, & m = 1 \\ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, & m > 1. \end{cases} \quad (10)$$

Based on (7), (9), and (10), one can show that V_{ix} and V_{iy} are independent of Δt. Therefore, to increase the efficiency, Δt can be assigned as unity.

When all the bus voltages are obtained, the power flow of each device is also calculated and (11) is used to calculate the security indices

$$S_{\mathrm{idx},k} = \min_{k=1}^{\mathrm{NB}} \{(P_{\mathrm{ijlmt}} - P_{ij,k})/P_{\mathrm{ijlmt}}\} \quad (11)$$

where NB is the number of branches, P_{ijlmt} is the active power limit of branch $i-j$, $P_{ij,k}$ is the power flow of the discretized case k, and $S_{\mathrm{idx},k}$ is the security index of the system.

B. Process Oriented Security Analysis

Suppose the initial time instant is t_0 and the contingency occurs at time t_f. Then the entire analysis interval $[t_0, t_e]$ is divided into $[t_0, t_f]$ and $(t_f, t_e]$. At time t_f, there is a failure which changes the structure or the parameters of the system. Hence the power flow equation is not continuous at this point. Mathematically, the derivative of power flow equation does not exist at t_f. However, this paper focuses on system state variations over a relatively large time scale, and hence, the transient process after

the contingency is ignored and the system is assumed as an inertial system, i.e.,

$$\begin{cases} V_{ix\cdot t_f-} = V_{ix\cdot t_f} = V_{ix\cdot t_f+} \\ V_{iy\cdot t_f-} = V_{iy\cdot t_f} = V_{iy\cdot t_f+}. \end{cases} \tag{12}$$

Therefore, by assuring t_0 as the initial point, the bus voltages of all the cases in the interval $[t_0, t_f]$ can be solved with the above mentioned Taylor series expansion method. Then we take t_{f+} as the initial point and the same method is used to obtain the bus voltages of all the cases in the interval $(t_f, t_e]$. The security index in the intervals can be calculated when the bus voltages of all the cases in the interval of $[t_0, t_e]$ are obtained. A summary of the procedures of the process-oriented security analysis is given in Appendix A.

C. $N-1-k$ Analysis and Cascading Failure Simulation

A disturbance and/or a device failure can affect the security of the power system. However, it is difficult to predict when and where a failure occurs since it depends on the internal, external or even anthropogenic factors of the power system. For example, equipment defects, apparatus overloading, extreme weather conditions or mis-operations can cause a failure. Thus, a great number of failures should be taken into account in a security analysis.

Although there are many causes for failures, an indisputable fact is that a large number of failures are caused by device overloading, especially in the case of continuous high load conditions, or when the system is subjected to a failure. Therefore, during the process-oriented security analysis, the status of the devices can be tracked after the initial $N-1$ fault and if the power flow of k device exceeds the limits, then the device can be assumed overloaded and tripped off by the protection. The outcome is that new failures have occurred and the security analysis program shifts to an $N-1-k$ analysis procedure. This process is repeated in the whole interval of the process-oriented security analysis either the end of the intervals or when the exit criteria are met. This process constitutes an $N-1-k\ldots$ rolling-forward security analysis process, and can provide a trend outlook for the power system security in the near future.

If the power flow of the faulted system, corresponding to the analysis of $N-1-k$, does not converge or the overloading at two adjacent cases exceeds a pre-specified amount, then the system can be considered to trigger a cascading failure and collapse after the first $(1+k+\ldots)$ failure. Therefore, a straightforward cascading failure simulation can be implemented through the process-oriented $N-1-k$ security analysis algorithm. The flow chart of the cascading failure simulation with a time-process oriented security analysis is shown in Fig. 2.

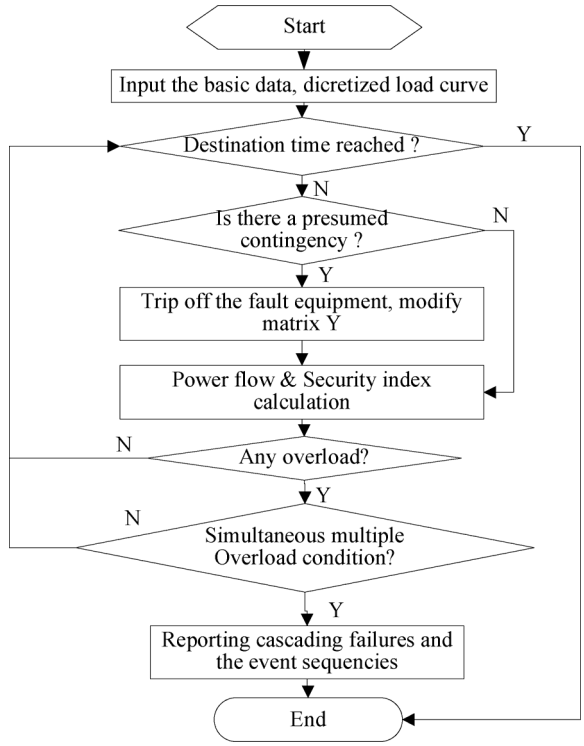

Fig. 2. Flow chart of a cascading failure simulation by a time-process-oriented security analysis method.

IV. Security Trend Analysis With Probabilities

The power system security is often evaluated subject to the most serious contingency. However, the most serious contingency should not necessarily be the main concern since its probability of occurrence is very low. It is not economical for the operation and control of the system to evaluate its security subject to the most serious scenario. Therefore, the security trend under different fault probability also should be considered.

Suppose there is a fault sets $\{C_{i,t}|i\in[1,M];t\in[t_0,t_e]\}$ which is formed by M independent contingencies. The subscript i of $C_{i,t}$ is the sequence number of the fault event and t is its occurrence time instant. Assume the occurrence probability of the events is $P(C_{i,t})$ which should satisfy Poisson distribution [32], i.e.,

$$P(C_{i,t}) = 1 - e^{-\lambda_{i,t}} \tag{13}$$

where $\lambda_{i,t}$ is the failure rate characteristic of the device i and can be determined based on historical records.

For a specific fault, the process-oriented security analysis method of Section III can be carried out and the security trend variations obtained. The trend variations describe the security level as a function of time, when the probability of the fault is 100%. Therefore, to present the fault occurrence probability and the corresponding system security level in the same coordinates, (14) is used as the probabilistic security indicator

$$S_{\mathrm{pid}}(t, C_{i,t}) = (1 - P(C_{i,t}))S_{\mathrm{idx}}(t, C_{i,t}) \tag{14}$$

where $S_{\mathrm{pid}}(t, C_{i,t})$ is the probability security index variation for contingency $C_{i,t}$. Expression $(1-P(C_{i,t}))$ indicates the probability that contingency $C_{i,t}$ does not occur. A larger value of this probability indicates a higher degree of security. If the probability of the contingency is fixed, then the security index $S_{\mathrm{idx}}(t, C_{i,t})$ determines the security level of the system. S_{pid} contains information regarding the probability of the contingency and the corresponding security level. Therefore, variations of $S_{\mathrm{pid}}(t, C_{i,t})$ fully demonstrates the trend of the system security under contingency $C_{i,t}$.

To describe the security trend of the power system more comprehensively and precisely, the trend boundary and trend channel should be defined. The upper boundary of the system security trend is defined as the security index profile obtained through the process-oriented power flow calculation in the intervals of $[t_0, t_e]$, where there is not any failures in the system, i.e.,

$$S_{\max} = S_{\mathrm{idx}}(t) \tag{15}$$

where $S_{\max}$ is the upper boundary of the security trend variation characteristic, $S_{\mathrm{idx}}(t)$ is formed by the connection of $S_{\mathrm{idx},k}$ as shown in (11), and $S_{\mathrm{idx},k}$ can be obtained based on the process-oriented power flow calculations. Obviously, the security trend characteristics of the power system are under the upper boundary during the operation. Similarly, the lower boundary of the power system security trend is defined by

$$S_{\min} = \left(\prod_{k=1}^{M}(1 - P(C_k))\right) \min_{i=1}^{N}\{S_{\mathrm{idx}}(t, C_{i,t})\} \tag{16}$$

where $S_{\min}$ is the lower boundary of the security trend characteristic and the first part of the formula is the probability that no contingency occurs in the fault set. Naturally, the security trend characteristics of the power system are above the lower boundary during the operation.

The upper and lower boundaries, in conjunction with the general probability trend characteristics, constitute the power system security trend channel. The security trend channel, which indicates the variation range of the system security level under all possible situations during the system operation, is a broad description of the system security trend. Therefore, during the system operation, the probability of contingent failures must be continuously analyzed to identify the security trend that is most likely to be deduced from the security trend channel.

V. Testing Scenario and Simulation Result

The IEEE 30-bus, 118-bus, and 300-bus test systems are used to evaluate the performance of the proposed method.

A. Construction of Bus Load Curves

Assume the system total load profile of each test system, within the time 6:30–22:45, is as shown in Fig. 3. The load is recorded every five minutes and hence there are 196 measurements between 6:30 and 22:45.

The load profiles can be reconstructed through a scaling process as follows:

- Firstly, select one point as the initial point in the profile and calculate the ratios of other measured values to this point.
- Secondly, calculate the total load of the test system and assume it is the initial system total load, and then scale it with the ratios to obtain the total system load for other measurements.
- Finally, according to the ratio of each load to the system total load, obtain the load of each bus at other measurement instants.

In this paper, the initial time instant of the IEEE 30-bus test system is set at 6:30, while the initial time instant of the other two systems is set at 13:20. In view of the lack of synchronism between each bus load and system total load, load profiles of some buses are adjusted subject to the condition that the system total load characteristic remains unchanged.

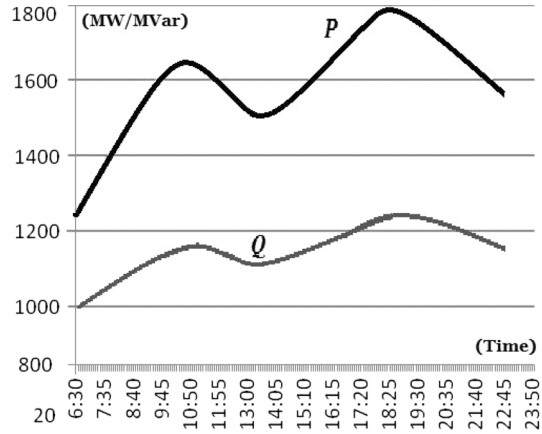

Fig. 3. Daily load variation characteristic of the test systems.

TABLE I
Comparison of the Computation Time Based on Different Methods (Milliseconds)

Test System	Newton-Raphson Method	Fast Decoupled Method	Method In This Paper
IEEE 30-Bus system	0.36	0.12	0.06
IEEE 118-Bus system	1.15	0.48	0.29
IEEE 300-Bus system	6.91	NC[1]	1.23

1. NC: Not Converged

B. Evaluation of the Taylor Series Expansion Power Flow

We calculate power flow at the 196 points in the interval of 6:30 to 22:45 with a Newton-Raphson method, a fast decoupled method and the Taylor series expansion method. For the Newton-Raphson and the fast decoupled methods, the processes are equivalent to calculating the power flows of 196 independent cases. Table I provides a comparison of the result.

Table I shows that the proposed method is noticeably faster than the traditional methods. The reason is that only linear constant-coefficient equations must be solved recursively and there is no need for iterative calculations of nonlinear equations. Therefore the method is highly effective for process calculations.

C. Evaluation of Process-Oriented Security Analysis

Suppose there are 4 contingencies which need to be analyzed for the IEEE 30-bus test system. The properties of the contingencies are shown in Table II.

For each contingency, the process-oriented analysis is carried out for the system and a security trend curve is obtained. As shown in Fig. 4, the security index (SI) of the system is reduced after each contingency. The reason is that the load transfer from the faulted device increases the load of other devices. Fig. 4 also reveals that the security index decreases as the system load increases, but not at the same rate. The reason is that the load in each bus changes with a different pattern and the pattern may

TABLE II
PROPERTIES OF THE FAULTS TO BE ANALYZED WITH PROCESS-ORIENTED METHODS

Contingency	Faulted Device	Bus I	Bus J	Time
Fault 1	T2	Bus-6	Bus-10	8:20
Fault 2	L6	Bus-2	Bus-6	13:30
Fault 3	L15	Bus-12	Bus-15	10:00
Fault 4	T1	Bus-6	Bus-9	19:30

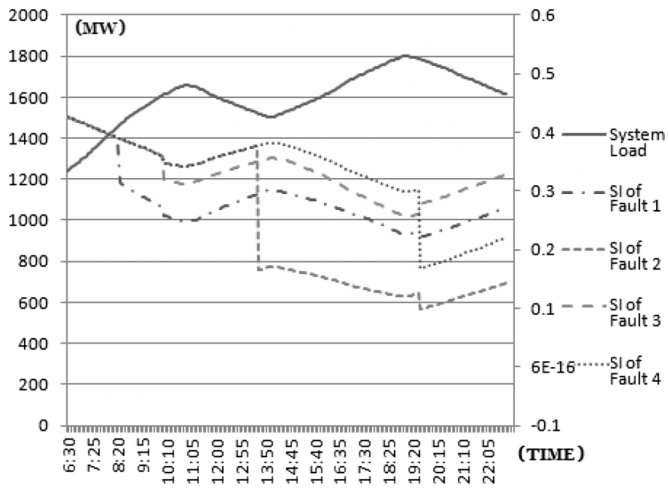

Fig. 4. Security indices with different faults of the IEEE 30-bus system.

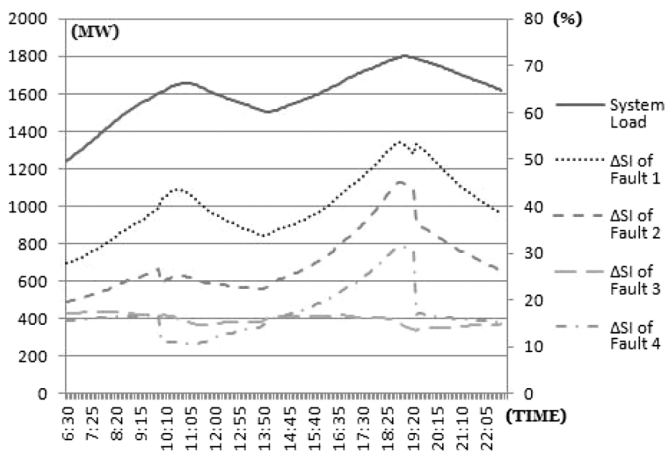

Fig. 5. Fault occurrence time via security indices of the IEEE 30-bus system.

differ from that of the total system load. Another interesting observation is that fault 3 which occurred near the first peak only leads to a slight drop of the security index, while the occurrence of fault 4 between the two peaks results in a significant drop of the security index. To clarify this phenomenon, another test, which provides a measure of the relationship between the fault occurrence time and the system security, is carried out in Fig. 5. Fig. 5 shows that the impact of the fault occurrence time on security and the system load is rather complex and not necessarily unison. This phenomenon also explains the reason that the security analysis result, based on the most serious case, is not necessarily reliable.

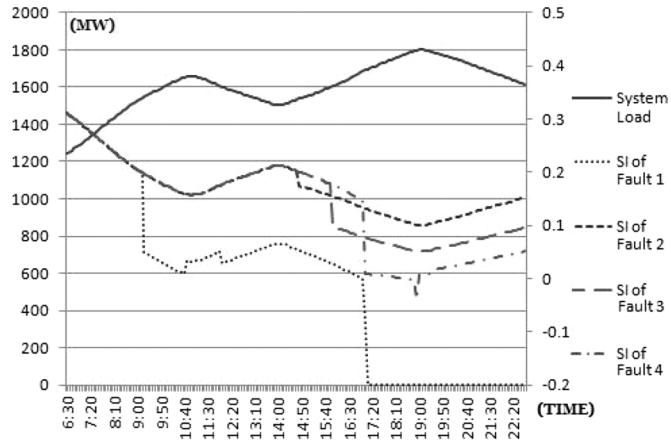

Fig. 6. Security indices of the IEEE 118-bus system $N-1-k$ analysis.

TABLE III
PROPERTIES OF THE FAULTS FOR $N-1-k$ ANALYSIS

Contingency	Faulted Device	Bus I	Bus J	Time
Fault 1	L30	Bus-23	Bus-25	9:10
Fault 2	L31	Bus-25	Bus-27	14:40
Fault 3	L62	Bus-42	Bus-49	15:50
Fault 4	L87	Bus-38	Bus-65	17:00

TABLE IV
$N-1-k$ ANALYSIS RESULTS OF THE IEEE 118-BUS SYSTEM

Contingency	New Fault	Time	New Faults	Consequence
Fault 1	Ln50	16:55	Ln173, Lnl9	Cascading
Fault 2	N/A	N/A	N/A	Secure
Fault 3	N/A	N/A	N/A	Secure
Fault 4	Ln50	17:35	Ln20	Secure

D. Evaluation of $N-1-k$ and Cascading Failure Simulation

The IEEE 118-bus test system is used to test $N-1-k$ analysis method. Four heavily loaded transmission lines, whose failures are expected to greatly affect the system security, are assumed to be contingent. The contingencies and the results are listed in Tables III and IV respectively. The security index variation of each fault is shown in Fig. 6.

Fig. 6 shows that the security index variations of fault 2, fault 3 and fault 4 are similar to those of Fig. 4. The reason is that no subsequent faults are caused by these faults. For fault 1, the security index characteristic drops significantly and then with the increase of the load to the peak value, Ln50 is overloaded and tripped off at 4:55 pm. Then Ln173 overloaded and tripped off, which leads to overloading of Ln19. After Ln19 is tripped off, the power flow solution cannot converge and a cascading failure is experienced. The occurrence of fault 5 also leads to overloading and tripping off of Ln50, and then leads to overloading and trip off of Ln20. Subsequently, with the decrease of the system load, the security index increases and no further overload is experienced. Therefore, fault 5 does not lead to a cascading failure.

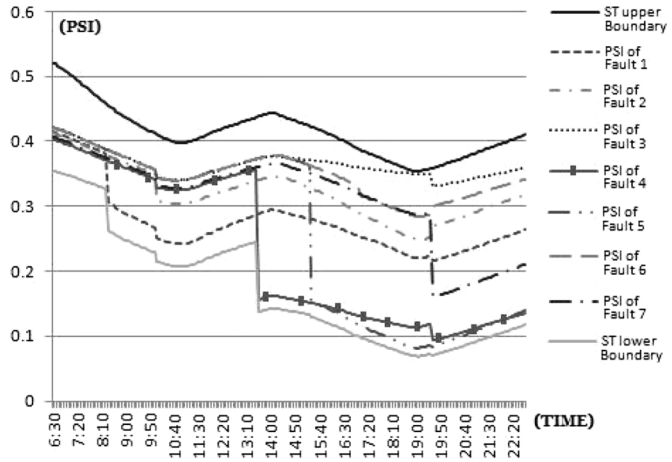

Fig. 7. Security trend channel of the IEEE 30-bus system.

TABLE V
PROPERTIES OF THE FAULTS TO BE STUDIED BASED ON PROBABILITY SECURITY TREND ANALYSIS METHODS

Contingency	Probability (%)	Faulty Device	Bus I	Bus J	Time
Fault 1	2.5	T2	Bus-6	Bus-10	8:20
Fault 2	3.1	L15	Bus-12	Bus-15	10:00
Fault 3	0.8	L20	Bus-18	Bus-19	11:50
Fault 4	5.2	L6	Bus-2	Bus-6	13:30
Fault 5	0.8	L25	Bus-10	Bus-22	15:20
Fault 6	1.0	L30	Bus-24	Bus-25	17:00
Fault 7	4.3	T1	Bus-6	Bus-9	19:30

E. Evaluation of Probability Security Trend Analysis

The probability model of the device failure is complex and deserves more in-depth research. In this section, the IEEE 30-bus system is used to test the concept of security trends with probabilities. The faults and their probabilities are listed in Table V. Fig. 7 shows the results based on the probability security trend analysis and the security index variations and the boundaries.

The security trend channel demarcates the variation range of the security trend in the interval. Therefore, based on such a diagram, the operator can get a wider view beyond the future security of the system during the operation.

VI. CONCLUSION

This paper introduces the concept, a methodology and a fast algorithm for trend-oriented security analysis of the power system.

In contrast to the traditional study-case-based analysis, the proposed security trend analysis method utilizes the load profile forecasts and contingency occurrence probability to calculate the security trend of the system in the subsequent time window. The method can be integrated as an $N-1-k$ analysis and used to investigate cascading failures. The trend-oriented security analysis is a "forward-looking" method and hence can determine the system security trend in advance. Thus, it can provide early warnings or control means to enhance the security of the power system.

The results of the test scenarios show that the proposed method is feasible and efficient. One can believe that further studies based on real systems can make the method more perfect and applicable.

APPENDIX A

The procedure of the process-oriented security analysis is summarized as follows.

- According to the forecasted load profile, discretize the analyzing interval $[t_0, t_e]$ into N calculating cases, where N is an integer number.
- Set the occurrence moment t_f of the presumed contingency and determines the corresponding case.
- Take t_0 as the initial point, set up the pre-fault power flow equation of the system as shown in (2).
- According to the voltage of the initial points, find out the Taylor series expansion of power flow equations as shown in (5)–(8).
- Solve the high order derivatives of voltage until the tolerance meets the pre-setting condition.
- Use (9) to calculate the node voltages.
- Repeat the process until voltages of all the cases between t_0 and t_f are obtained.
- Let t_{f+} as the initial point of the sub-process after the contingency, set up the post-fault power flow equation according to the type of the contingency.
- Solve the power flow of all the post-contingency cases with the Taylor series expansion method.
- Calculate the security indices of all the cases, and visualize the indices as the security trend characteristic.

REFERENCES

[1] IEEE/CIGRE Joint Task Force on Stability Terms and Definitions, "Definition and classification of power system stability," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 1378–1401, May 2004.

[2] M. Shahidehpour, W. F. Tinney, and Y. Fu, "Impact of security on power systems operation," *Proc. IEEE*, vol. 93, no. 11, pp. 2013–2025, Nov. 2005.

[3] P. Kundur, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 1994, p. 135.

[4] C. Pang and M. Kezunovic, "Static security analysis based on weighted vulnerability index," in *Proc. 2011 IEEE Power and Energy Society General Meeting*, pp. 1–6.

[5] E. Ciapessoni, D. Cirio, S. Grillo, S. Massucco, A. Pitto, and F. Silvestro, "An integrated platform for power system security assessment implementing probabilistic and deterministic methodologies," in *Proc. 2010 Complexity in Engineering*, pp. 40–42.

[6] R. Liu, J. Zhang, W. Qiu, L. Su, Z. Guo, and G. Wang, "Research on online static risk assessment for urban power system," in *Proc. 2010 Power and Energy Engineering Conf.*, pp. 1–4.

[7] D. Chatterjee, J. Webb, Q. Gao, M. Y. Vaiman, M. M. Vaiman, and M. Povolotskiy, "N.-1.-1. AC contingency analysis as a part of NERC compliance studies at midwest ISO," in *Proc. 2010 IEEE PES Transmission and Distribution Conf. Expo.*, pp. 1–7.

[8] N. Fan, R. Chen, and J.-P. Watson, "N.-1.-1. contingency-constrained optimal power flow by interdiction methods," in *Proc. 2010 IEEE Power and Energy Society General Meeting*, pp. 1–6.

[9] M. Rahnamay-Naeini, Z. Wang, A. Mammoli, and M. M. Hayat, "A probabilistic model for the dynamics of cascading failures and blackouts in power grids," in *Proc. 2012 IEEE Power and Energy Society General Meeting*, pp. 1–8.

[10] R. Fitzmaurice, E. Cotilla-Sanchez, and P. Hines, "Evaluating the impact of modeling assumptions for cascading failure simulation," in *Proc. 2012 IEEE Power and Energy Society General Meeting*, pp. 1–8.

[11] Y. Zheng, W.-Y. Liu, Z.-W. Wen, and D.-M. Ping, "A real-time searching system for cascading failures based on small-world network," in *Proc. 2010 Power and Energy Engineering Conf.*, pp. 1–5.

[12] F. Ren, M. Zhang, D. Soetanto, and X. D. Su, "Conceptual design of a multi-agent system for interconnected power systems restoration," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 732–740, May 2012.

[13] J. Yu, L. Yang, R. Liu, and Z. Guo, "Research on time process-oriented power system static security analysis," in *Proc. 2008 3rd Int. Conf. DRPT*, pp. 1516–1521.

[14] Y. Jiaxi, G. Zhizhong, B. Xuefeng, and L. Ruiye, "Power system static security analysis with time process-oriented method," *Trans. China Electrotech. Soc.*, vol. 25, no. 10, pp. 142–149, Oct. 2010.

[15] W. Lian, A. Mao, L.-Z. Zhang, S. Zhao, and D. Zhang, "A method for cascading failure simulation based on static security analysis," in *Proc. 2009 Asia-Pacific Power and Energy Engineering Conf.*, pp. 1–5.

[16] J. Schannep, *Dow Theory for the 21st Century: Technical Indicators for Improving Your Investment Result*. Hoboken, NJ, USA: Wiley, 2008, pp. 1–55.

[17] Y. Xiong, S. Guo, and S. Guan, "An application of RBF neural network method for the price tendency of Europe Brent crude oil," in *Proc. 2007 the 2nd Int. Forum Chinese Energy Strategy*, pp. 1–6.

[18] M. W. Covel, *Trend Following: How Great Traders Make Millions in Up or Down Markets*. Englewood Cliffs, NJ, USA: Financial Times Prentice Hall, 2006.

[19] A. T. C. S. Jeffrey and J. Woell, "Application of trend analysis methodologies on built-in-test (BIT) (and non-BIT) systems in a operational U.S. navy fighter/attack squadron," in *Proc. 2005 Instrumentation and Measurement Technology Conf.*, Ottawa, ON, Canada, pp. 1836–1841.

[20] S. M. Glista, D. J. Rushing, and C. R. Lide, "F-22 subsystem fleet management trend analysis," in *Proc. 2010 ASME International Mechanical Engineering Congr. Expo.*, vol. 5, pp. 251–266.

[21] L. Peirlinck, P. Guillaume, and R. Pintelon, "Accurate and fast estimation of the fourier coefficients of periodic signals disturbed by trends," *IEEE Trans. Instrum. Meas.*, vol. 45, no. 1, pp. 5–11, Feb. 1996.

[22] J. Wang, D. Chi, and J. Wu, "Chaotic time series method combined with particle swarm optimization and trend adjustment for electricity demand forecasting," *Expert Syst. Applicat.*, vol. 38, no. 7, pp. 8419–8429, Jul. 2011.

[23] E. González-Romera, M. Á. Jaramillo-Morán, and D. Carmona-Fernández, "Monthly electric energy demand forecasting based on trend extraction," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1946–1953, Nov. 2006.

[24] K. Siwek, S. Osowski, and B. Swiderski, "Trend elimination of time series of 24-hour load demand in the power system and its application in power forecasting," *Przegląd Elektrotechniczny*, vol. 87, no. 3, pp. 249–253, 2011.

[25] R. Moghe and M. J. Mousavi, "Trend analysis techniques for incipient fault prediction," in *Proc. 2009 IEEE Power & Energy Society General Meeting*, pp. 1–8.

[26] C. J. Kim, "Identification of symptom parameters for failure anticipation by timed-event trend analysis," *IEEE Power Eng. Rev.*, pp. 48–49, Sep. 2000.

[27] L. Peretto, R. Sasdelli, and R. Tinarelli, "A statistical model for estimating the trend of electrical quantities in power systems," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 4, pp. 1143–1147, Aug. 2003.

[28] C. León, F. Biscarri, I. Monedero, J. I. Guerrero, J. Biscarri, and R. Millán, "Variability and trend-based generalized rule induction model to NTL detection in power companies," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 1798–1807, Nov. 2011.

[29] A. R. Messina and V. Vittal, "A structural time series approach to modeling dynamic trends in power system data," in *Proc. 2012 IEEE Power & Energy Society General Meeting*, pp. 1–8.

[30] A. R. Messina, V. Vittal, G. T. Heydt, and T. J. Browne, "Nonstationary approaches to trend identification and denoising of measured power system oscillations," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1798–1806, Nov. 2009.

[31] A. A. Fouad, S. Venkataraman, and J. A. Davis, "An expert system for security trend analysis of a stability-limited power system," *IEEE Trans. Power Syst.*, vol. 6, no. 3, pp. 1077–1084, Aug. 1991.

[32] W. Li, *Risk Assessment of Power Systems: Models, Methods and Applications*. New York, NY, USA: Wiley, 2005, pp. 227–228.

Anjia Mao was born in Xishui, Hubei province, China, on August 28, 1975. He graduated from Harbin Institute of Technology (HIT) and continued his post-graduated education in HIT. He received the Ph.D. degree in engineering in July 2006.

He is now an Associate Professor at North China Electric Power University and a visiting professor at the University of Toronto, Canada. His current main research interests focus on power system security analysis and control, power system dynamic, power system automation, and electricity market. His employment experience includes a system designer in the Dong Fang Electronic Information Industry Co. Ltd., YanTai, China, from July 2000 to March 2003. His special fields of interest include energy manage system.

M. Reza Iravani (M'85–SM'00–F'03) received the B.Sc. degree in 1976 from Amirkabir University of Technology (Tehran Polytechnic), Iran, and the M.Sc. and Ph.D. degrees from the University of Manitoba, Winnipeg, MB, Canada, in 1981 and 1985, respectively.

He is a Professor in the Edward S. Rogers Sr. Department of Electrical and Computer Engineering at the University of Toronto, Toronto, ON, Canada. His research interests include application of power electronics in electric power systems, modeling and analysis of electromagnetic transient phenomena in power systems, and power system dynamics and control.