Comparing Security Assessment Schemes Through Two-Stage Monte Carlo Sampling

James Brooks
Electrical and Electronic Engineering
University of Bath
Bath, UK. BA2 7AY
Email: j.brooks@bath.ac.uk

Rod Dunn
Electrical and Electronic Engineering
University of Bath
Bath, UK. BA2 7AY

***Abstract*—The penetration of unscheduleable generation will increase due to legislation and eventually saving on fuel cost. This will cause an increase in uncertainty of power flow and drive up balancing market costs. A security assessment scheme that considers probabilistic uncertainty could give financial savings and better security of supply.**

Any change in security assessment scheme must be tested, compared, and verified. Though there has been a lot of work into probabilistic security assessment there has been far less on comparing security assessment schemes. This work uses two stage Monte Carlo sampling to generate a data set which can be used for easy comparison between different schemes.

In this paper numerical results are presented that show that this method can provide valuable information about how the system will cope with unexpected changes. This will allow security assessment schemes to be developed in the future that do not disadvantage a high penetration of variable renewable generation.

***Index Terms*—Monte Carlo methods, Power system reliability, Power system security, Power system simulation, IEEE Reliability Test System, Sustainable Power Generation**

I. Introduction

Reliable operation of electric power systems is taken for granted across most of the developed world. But this reliability is far from guaranteed; an electric power system can be seen of as one of the largest and most complicated machines ever created. The decentralisation of power markets has caused power system to be driven closer to their operation limits, trading off security for cost. The optimal way to do this trade-off is by having the most accurate security assessment schemes available.

If a sub-optimal security assessment scheme is used it may lead to costly over-securing in certain conditions and dangerously low security in others. This will mean that higher safety margins must be put on the poor security scheme which will lead to an unnecessarily high cost. An accurate scheme should take into account both likelihood and consequence of every possible event. In fact a security assessment scheme should accurately represent the risk of running the system in the current state where risk is a function of likelihood and consequence for every possible event [1].

$$R = \sum_i L(e_i) \times C(e_i) \tag{1}$$

Where R is Risk, e is an event, L is likelihood, and C is consequence.

A perfect system is infeasible in practice due to time constraints. In the UK, system operators have only one hour to perform final balancing actions between the FPN - the point when they are supplied with the final load/generator data, and the point of delivery. Though the balancing market lasts only one hour, the system operator is likely to make predictions on generator bids beforehand for use in preliminary calculations. Power system security is all about coping with likely changes, Kirschen [2] provides a good overview to some of the challenges involved these include:

- Maintaining good **power quality**, i.e. that the voltages/currents are approximately sine-waves at 50Hz.
- Keeping system **synchronism**, i.e. that every generator is approximately at the same frequency and phase.
- Requested power being delivered to most loads, i.e. **no load shedding**
- Keeping each component **within limits** for voltage/current/power most of the time (i.e. there are no components that are overloaded or experiencing voltage collapse).
- Making the system reasonably **fault tolerant**.
- Suppling energy at **minimum cost** with **minimum environmental impact**.

Obviously from the above list security cannot easily be defined in absolute terms; the trade-off between being fault tolerant and cost shows this. The goal is to achieve an acceptable level of security at least cost. To deal with the massive complexity involved in this calculation many simplifying assumptions are made and the use of computer simulations is invaluable.

Various types of computer simulation can be run to determine the behaviour of the system. These include a *load flow*, a *dynamic simulation* and a *transient simulation*. Each of these tests considers the system in increasing levels of complexity; the transient simulation is the most accurate but slowest test to run.

This paper uses the definition in [3] where reliability is the long term ability to safely and securely supply the demand for power. Secure operation is a power system's ability to remain stable and within operational limits following any

likely disturbance. And stability refers to the whether the system can regain a state of operational equilibrium following a specific disturbance. For a broad overview of the method used within power system reliability refer to the works of Billinton and Allen [4].

A. Deterministic Power System Security

Traditionally, security assessment schemes manage this complexity by using a set of credible contingencies. These are meant to represent all likely events with a severe consequence. In other words they should be events with the largest product of likelihood and consequence. There has been significant work into determining which events to include [5] [6] [7]. These contingencies are often different for each half hour delivery period and vary based upon weather and season.

The set of normal contingencies that are considered is given in [8]; a subset of this is known as *N-1*. N-1 is a security assessment scheme that considers the failure of one component (line, generator or transformer) at a time. In other words, the simultaneous failure of two components is considered too unlikely to count. There have been various modifications to N-1 including the addition of correlated failures, such as the failure of two lines on a common right-of-way.

The UK system operator does consider a subset of N-2 contingencies where two simultaneous failures are considered but not all possible double failures are checked. This traditional contingency screening has worked well for many years but with the paradigm shift in generation that is coming in the form of local, unscheduleable generation it is time to review this idea.

The problem with all such N-x methods (N-1, N-2, etc.) is that they treat likelihood in such a crude way; it assumes all contingencies to be equally likely.

Another such disadvantage of any deterministic security assessment scheme is that it can lead to problems if something outside of the expected set happens. In the UK the simultaneous failure of two generators was considered non-credible; hence, after it occurred during 2008, emergency operator action was needed. This is far from the only incident of its kind. 2003 saw more than it's fair share of major incidents with North America, Libya, London and Italy [9] all experiencing widespread blackouts.

The credible disturbances are no longer best represented by discrete events. The change in wind power over a one hour period is significant, spatially correlated and continuous. It is possible to treat wind power as a contingency by quantizing it at a large resolution into a small number of likely states. In performing this method one must be careful to have enough possible wind states to accurately represent everything that could happen.

If wind farms continue to be built at the current rate wind power will become a major component of the UK's plant mix. Unless the market changes this is likely to disadvantage wind farms due to their uncertainty [10]. Some may say that their cost will accurately reflect their difficult of incorporating such uncertainty in a power system but there is no point in building wind turbines if they are not to be fully utilised. Renewable power should be encouraged from an environmental point of view however the technical challenges must be overcome. In reality the likelihood is that the wind resource as a whole will not fluctuate drastically, especially if turbines are distributed over a large geographical area. But the risk must be quantified and verifiable before new security assessment methods can be implemented.

B. Probabilistic Power System Security

Risk based (probabilistic) security assessment uses probability much more directly. It is not a new idea it has been used in other industries since the 1960's; and has been studied in power systems since the 1970's [11]. But it is computationally expensive and often harder to produce a verifiable result. As the disadvantages of deterministic methods impacts financially, the focus has begun to turn towards probabilistic methods [6] [2]. This is already happening as balancing market prices have been driven up by wind power [10].

Sobajic et. al. [12] provides a brief overview of four different approaches to the problem of stability assessment. The paper then discusses one such pattern recognition method after highlighting the works of Patton, Billinton, and Wu as contributing significantly to probabilistic methods.

After an extensive literature review, including the mention of Monte Carlo methods, McCalley [13] goes on to determine a set of deterministic rules based upon risk based methods.

Monte Carlo methods are a type of algorithm used commonly in risk assessment where a system with uncertainty is repeatedly sampled. In this way Monte Carlo Methods lend themselves well to the task of probabilistic risk assessment. A comparison of different modifications to standard Monte Carlo Methods is given in [14], there a financial value is placed upon outages to give an absolute level of comparison.

For an up-to-date review of the work in risk based security assessment see [15]. It also provides a good conceptual representation which shows how risk based security assessment will more accurately reflect the actual level of security. Xiao [16] shows graphically how traditional SCOPF can produce a more risky solution due to it's fixed constraints.

By assigning a severity to each type of disturbance Ni [17] created a system for aiding control room decisions based on risk.

C. Comparing Security Assessment Schemes

Although there is significant work on different types of security assessment scheme and how well they perform there is relatively little work performing a direct comparison between two such schemes. Any new scheme must fit a number of criteria most importantly it must not decrease the level of reliability or increase the cost. This is the main requirement of a security assessment scheme, but there are other criteria that must be considered. The scheme must be verifiable, that is, following an incident, it should be possible to determine who is at fault; the operator, the security assessment scheme or was it an anomalous event that requires no improvement

to be made. It must be able to be used within the time-frame of 1 hour, remembering that this time includes making necessary modifications and re-running the test until the system is adequate. Finally it must not unfairly disadvantage any particular generator and ideally should allow for the most environmentally friendly operation (by not curtailing renewables).

D. The IEEE Reliability Test System 96

The IEEE-RTS is a sample power system with a thorough set of data for operation, emissions, and reliability. It was for this reason that it was chosen as the test system for this work. Only area A was used, which is composed of 32 generating units, 24 busbars, 38 lines, 17 loads and two voltage levels.

TABLE I
LINE PROBABILITIES

Line ID	From	To	Fail Rate	MTTR
A1	1	2	0.24	16
A2	1	3	0.51	10
A3	1	5	0.33	10
A4	2	4	0.39	10
A5	2	6	0.48	10
A6	3	9	0.38	10
A7	3	24	0.02	768
A8	4	9	0.36	10
A9	5	10	0.34	10
A10	6	10	0.33	35
A11	7	8	0.30	10
A12-1*1	8	9	0.44	10
A13-2*1	8	10	0.44	10
A14	9	11	0.02	768
A15	9	12	0.02	768
A16	10	11	0.02	768
A17	10	12	0.02	768
A18*2	11	13	0.40	11
A19	11	14	0.39	11
A20*2	12	13	0.40	11
A21	12	23	0.52	11
A22	13	23	0.49	11
A23	14	16	0.38	11
A24	15	16	0.33	11
A25-1*3	15	21	0.41	11
A25-2*3	15	21	0.41	11
A26	15	24	0.41	11
A27	16	17	0.35	11
A28	16	19	0.34	11
A29	17	18	0.32	11
A30*4	17	22	0.54	11
A31-1*5	18	21	0.35	11
A31-2*5	18	21	0.35	11
A32-1*6	19	20	0.38	11
A32-2*6	19	20	0.38	11
A33-1*7	20	23	0.34	11
A33-2*7	20	23	0.34	11
A34*4	21	22	0.45	11

* starred lines are on a common right of way with those of the same number if one fails the other will also fail with a probability 0.08

II. METHODOLOGY

The work is based around a two stage Monte Carlo Sampler which uses a Matlab PSAT simulation of the IEEE-RTS Area 1. The first stage generates *scenarios*, representing possible states the power system could be in. The second stage is used to create the probability that each of the scenarios from the first stage are acceptable. In this context acceptable means that no emergency operator action is required during the half-hour delivery period. This data is then tabulated to form an overall picture of how secure the system is in a number of cases. This can be useful in its own right but it can be further used to compare security assessment schemes as described below. The outline for this process is given in 1.

TABLE II
GENERATOR PROBABILITIES

Generator ID	Bus	MTTF	MTTR
G1	1	450	50
G2	1	450	50
G3	1	1960	40
G4	1	1960	40
G5	2	450	50
G6	2	450	50
G7	2	1960	40
G8	2	1960	40
G9	7	1200	50
G10	7	1200	50
G11	7	1200	50
G12	13	950	50
G13	13	950	50
G14	13	950	50
G15	14	-1	-1
G16	15	2940	60
G17	15	2940	60
G18	15	2940	60
G19	15	2940	60
G20	15	2940	60
G21	15	960	40
G22	16	960	40
G23	18	1100	150
G24	21	1100	150
G25	22	1980	20
G26	22	1980	20
G27	22	1980	20
G28	22	1980	20
G29	22	1980	20
G30	22	1980	20
G31	23	960	40
G32	23	960	40
G33	23	1150	100

A. Monte Carlo Stage One

1) Rationale: Stage one consists of sampling to generate a range of realistic operating conditions. These are meant to be a representative sample of the possible states of the power system after the system operator has performed some balancing actions. If this method was applied to a real system, and the data was available, historic information for the system in question could be used, but as the RTS is a theoretical system no such data was available.

To represent the possible states: outages, forecasts and operator actions should all be considered. As these are correlated a realistic set of data is hard to come by, the RTS provides such data. Below is a list of some of the factors that could be considered:

- Faulted components on outage for repair
- A load forecast based upon date and time

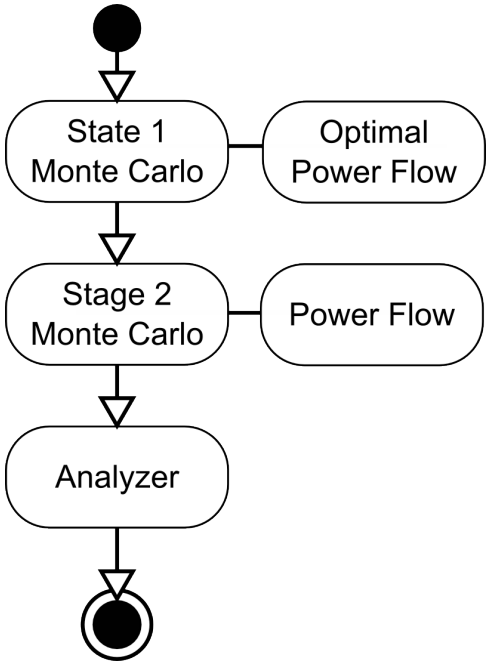

Fig. 1. Structure of Comparison Program

- A weather forecast giving the output power of renewable generators
- The effects of sympathetic tripping and common right of way failures
- Bid & offer prices for all scheduleable generators
- System operator balancing actions

2) Implementation: Not all factors are considered in this work, outages of lines busbars and generators are calculated from their mean time to fail (MTTF) and mean time to repair (MTTR) as per equation 2. For components that have a failure rate specified instead of a MTTF a simple conversion was performed. Busbar failure rate is not included in the original paper so a value of 0.025 was chosen to be consistent with values in the literature. Failure rate is given in failures per year and MTTF and MTTR is given in hours. Included in the paper is the probability that the tripping of certain lines will cause tripping of others, this effect was also taking into account in this work.

$$P_o = \frac{MTTF}{(MTTF + MTTR)} \tag{2}$$

3) Theoretical Results: As a test for the Monte Carlo sampling, shown later, a simple calculation of the expected number of failures per component was performed. This simply uses the average outage probability multiplied by the number of components. The expected number of failures given in III should approximately match the results obtained from the Monte Carlo Sampling in the next section.

4) Monte Carlo Results: One million samples were run and it can be seen that the theoretical and Monte Carlo results match to within a few percent. It should be noted that lines can also fail because of correlated common right of way failures.

TABLE III
THEORETICAL RESULTS

Name	No.	Min	Max	Average
Bus P_o	24	3.70E-005	3.70E-005	3.70E-005
Bus P_f	24	3.00E-006	3.00E-006	3.00E-006
Line P_o	38	3.42E-004	1.75E-003	6.69E-004
Line P_f	38	2.00E-006	6.20E-005	3.90E-005
Generator P_o	32	1.00E-002	1.20E-001	4.34E-002
Generator P_f	32	3.40E-004	2.22E-003	8.80E-004

TABLE IV
COMPARISON OF THEORETICAL AND MONTE CARLO RESULTS IN 1,000,000 SAMPLES

Name	Theoretical	Monte Carlo	% Error	Abs Error
Bus P_o	888	861	0.030	27
Bus P_f	72	65	0.097	7
Line P_o	25110	25117	0.000	7
Line P_f	1481	1441	0.027	40
Generator P_o	758554	764102	0.007	5548
Generator P_f	27779	27657	0.004	122

For this reason the line outages are expect to differ more than the other components. It is likely due to the low probability of this tripping type that it is not noticed in the final results.

5) Further work - system operator and power system simulation: Although the work completed to date does not include it, a simulated system operator is necessary to take the outages and forecasts into a viable system. In reality a system operator would have been planning constraints and contingencies for a long time before delivery. The full effect of a system operator is not something that can be modelled accurately by a computer. But at it's minimum a pool system can be assumed and generator outputs can be set to minimise cost. This will lead to overly unsecured systems but for the purposed of this work a wider range of security is of no disadvantage.

An enhancement to pool system economic dispatch is to consider the stability or even the security of the final system. This does lead to a problem: How can you compare different security schemes when you are using a security scheme as part of the testing procedure. The simplest way to overcome this is to use a range of different schemes. It is not required that each of the scenarios could be used under any particular security assessment scheme. What is required is that a wide range of possibilities are shown.

B. Monte Carlo Stage Two

1) Rationale: The second stage takes each scenario through another round of Monte Carlo sampling. This time it samples for unplanned changes, these include:

- Load forecast error
- Weather forecast error hence generator power mismatch
- Component faults during current operation period (of 0.5 hour)

The purpose of this stage is to see what realistically might happen to a power system in such a state. By simulating each

of these samples we can obtain a measure of how likely it is that the given scenario will need emergency operator action and hence one measure of security level.

2) Implementation: Load forecast error is consider but only in the most basic form, a normally distributed random number with mean 1 and s.d. 0.05 is multiplied by the forecast given in stage one. A more realistic measure should take better account of the correlation between time and load forecast error as well as weather impacts. Component faults are taken by converting line, generator and busbar value (from the original paper), into the probability that they will fault during the half hour delivery period, this uses equation 3. As the IEEE-RTS does not have renewable generators a weather forecast is unnecessary.

$$P_f = 1 - e^{-\lambda t} \tag{3}$$

3) Results: Again theoretical results were calculated to verify the implementation of the Monte Carlo sampling program, these results are given in table IV. The result for the Monte Carlo and theoretical match up very well showing the implementation is correct.

4) Further Work - power system simulation and automatic actions: The simulation of the second stage is less involved than the first. Because we are looking for systems where emergency operator action is not needed we do not have to simulate a system operator for this stage. This means only automatic actions need to be modelled, the ideal method for this is to do a full dynamic simulation. Starting from the scenario and adding each of the changes when the previous changes' oscillations have damped down.

As millions of simulations are likely to be required either distributed computing or a change to the simulator will be required. A load flow simulation is an order of magnitude faster than a dynamic simulation but does not have the ability to model outages and mismatches in the same way.

Once the simulations are performed and acceptable systems are marked as such we can move on to the analysis stage.

C. Analysis Stage

This leads to the final section of the method, performing the comparison between different security assessment schemes. A perfect security assessment scheme would only pass those states where the probability of the system remaining acceptable was above a certain threshold. This threshold is a trade-off between the extra cost of securing the system and penalties caused by unsupplied load. It would be highly system dependent and it's calculation is not covered by this paper.

The first two parts of this work have given an approximation for the probability of acceptability for a number of different scenarios. If these are plotted as in 2 each security assessment scheme can simply be run with each of the scenarios to see if it agrees with the theoretical ideal. The sample data in 2shows that the top item was in error more then the bottom one. This means that the bottom one is a better security scheme for this system. It would also be interesting to know which cases are in error. If they are near to the threshold then it is less severe than if they are far away.

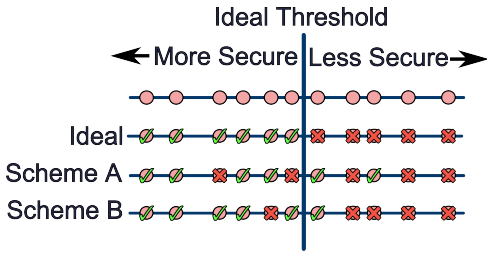

Fig. 2. Comparing Security Assessment Schemes

III. Limitations

This method allows two security assessment schemes to be compared but it does suffer from limitations. These limitations do not remove its merit but should be considered in future applications of this method.

- These is a significant data requirement. Some power systems will not have sufficient data to create the Monte Carlo model.
- These is a significant computational requirement. Many millions of power system simulations are required.
- The proposed method requires a simulated system operator, this is very difficult to accurately achieve.
- Any non-deterministic simulation has a chance of giving misleading results through insufficient samples.
- This method does not aim to make general claims about the ability of different security assessment schemes.
- Counting of unlikely events means things that were not included in the Monte Carlo could have a greater affect.
- The method does not distinguish between severity of failure. Both a small overload on a line and a system-wide blackout are considered the same.

It is the intention of the authors to further refine the proposed method to mitigate some of the limitations.

IV. Conclusion

In this paper a method for comparing security assessment schemes was introduced. Initial results test the implementation of the two stage Monte Carlo sampler showing a high correlation with expected results.

It is explained how this two stage Monte Carlo could be extended using simulation to provide a framework to easily compare security assessment schemes. Although there are many challenges and limitations to the method if these can be overcome it will provide a valuable tool to system operators.

Acknowledgement

This work was funded by Supergen.

References

[1] R. Billinton, L. Salvaderi, J. McCalley, H. Chao, T. Seitz, R. Allan, J. Odom, and C. Fallon, "Reliability issues in today's electric power utility environment," *Power Systems, IEEE Transactions on*, vol. 12, no. 4, pp. 1708–1714, Nov 1997, done, initial.

[2] D. Kirschen, "Power system security," *Power Engineering Journal [see also Power Engineer]*, vol. 16, no. 5, pp. 241–248, Oct 2002, done, initial. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs$_all.jsp?arnumber = 1106706$

[3] J. A. V. A. G. B. A. C. C. H. N. H. D. S. A. T. C. V. C. T. V. V. Kundur, P. Paserba, "Definition and classification of power system stability," *Power Systems, IEEE Transactions on*, vol. 19-3, pp. 1387 – 1401, 2004.

[4] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*, Plenum, Ed. Springer, 1996, no. ISBN:0306452596. [Online]. Available: http://books.google.co.uk/books?id=b6I4MdiVgn8C

[5] N. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M. Lauby, B. Wollenberg, and J. Wrubel, "On-line power system security analysis," *Proceedings of the IEEE*, vol. 80, no. 2, pp. 262–282, Feb 1992, done, initial.

[6] J. McCalley, V. Vittal, and N. Abi-Samra, "An overview of risk based security assessment," *Power Engineering Society Summer Meeting, 1999. IEEE*, vol. 1, pp. 173–178 vol.1, Jul 1999, done, initial.

[7] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, "Severe multiple contingency screening in electric power systems," *Power Systems, IEEE Transactions on*, vol. 23, no. 2, pp. 406–417, May 2008, done, initial.

[8] P. Kundur, *Power System Stability and Control*, E. P. S. Engineering, Ed. McGraw-Hill Professional (1 Mar 1994), 1994, iSBN 978-0070359581. [Online]. Available: http://www.amazon.co.uk/exec/obidos/ASIN/007035958X

[9] R. R. M. B. J. El-werfelli, M. Dunn, "Analysis of the national 8th november 2003 libyan blackout," *Universities Power Engineering Conference, 2008. UPEC 2008. 43rd International*, vol. 1, pp. 1–5, 2008.

[10] BWEA, "Wind power and intermittency: The facts," BWEA, Tech. Rep., 2005. [Online]. Available: http://www.bwea.com/pdf/briefings/intermittency-2005.pdf

[11] A. Patton, "A probability method for bulk power system security assessment, i-basic concepts," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-91, no. 1, pp. 54–61, Jan. 1972.

[12] D. Sobajic and Y.-H. Pao, "Artificial neural-net based dynamic security assessment for electric power systems," *Power Systems, IEEE Transactions on*, vol. 4, no. 1, pp. 220–228, Feb 1989, done, initial.

[13] J. McCalley, A. Fouad, V. Vittal, A. Irizarry-Rivera, B. Agrawal, and R. Farmer, "A risk-based security index for determining operating limits in stability-limited electric power systems," *Power Systems, IEEE Transactions on*, vol. 12, no. 3, pp. 1210–1219, Aug 1997, done, initial.

[14] K. Bell, D. Kirschen, R. Allen, and P.Kelen, "Efficient monte carlo assessment of the value of security," *Power Systems Computational Conference*, vol. 13th, p. ?, June 1999, done, initial. [Online]. Available: http://www.eee.strath.ac.uk/ kbell/publications.htm

[15] D. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *Generation, Transmission & Distribution, IET*, vol. 1, no. 4, pp. 527–533, July 2007, done, initial.

[16] F. Xiao and J. McCalley, "Risk-based security and economy tradeoff analysis for real-time operation," *Power Systems, IEEE Transactions on*, vol. 22, no. 4, pp. 2287–2288, Nov. 2007, done, initial.

[17] M. Ni, J. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *Power Systems, IEEE Transactions on*, vol. 18, no. 1, pp. 258–265, Feb 2003, done, initial.