Analyzing Security Assessment Schemes In Traditional Networks

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 introduction of sustainable and renewable energy sources into traditional networks will be limited if we continue to use inappropriate methods for security analysis. The probabilistic nature of variable and non-schedulable renewable generation is not well represented in current on-line security assessment schemes.**

This paper presents a novel method of analyzing and comparing system security schemes and provides initial results of one such scheme. It does so by dynamic simulation of Monte Carlo samples on the IEEE Reliability Test System (IEEE-RTS). It aims to provide information on both how often and how badly the system security scheme fails.

After testing on the IEEE-RTS it can be shown that there are credible failures that N-1 does not consider. It highlights the need for a new security assessment scheme that goes beyond a small deterministic set of test cases.

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

I. Introduction

The NERC Planning Standards [1] provide a commonly cited definition for security and adequacy. Security being the ability of the electric system to withstand disturbances. Whereas, adequacy is the ability to supply the total demand taking into account outages [2]. These are the two component parts of reliability: adequacy being a planning issue and security being an operational one.

The task in security control is to keep the system in the normal state. The normal state is defined as having all system variables within acceptable limits, that the system operates securely and it is able to withstand a contingency without violating the constraints [3]. Security assessment is the analysis of data from security monitoring. In this paper a method for comparing security assessment schemes is given.

Traditionally, security assessment schemes are based upon the simulation of a set of credible contingencies; The set of normal contingencies is given in [3]. This can lead to problems if something outside of the expected set happens. In the UK the simultaneous failure of two distant generators was considered non-credible; hence, after it occurred during 2008, emergency operator action was needed. With increasingly large and stressed systems the problem is intensified.

Additionally, the set of credible disturbances is no longer discrete. This means the contingency analysis itself is losing some of it's past merit. In the case of wind generation the output is stochastically variable, by treating it as a contingency you ignore the fact that the output can vary continuously between it's rate capacity and zero power output. Using traditional security assessment will increasingly disadvantage renewable generation as penetration grows [4]. In reality the likelihood is that national wind power as a whole will not fluctuate drastically, especially if turbines are distributed over a large geographical area [5]. But the risk must be quantified and verifiable before new security assessment methods can be implemented.

The definition of security in [6] gives further insight into the problem:

> Security may be defined as the probability of the system's operating point remaining in a viable state, given the probabilities of changes in the system (contingencies) and its environment (weather, customer demands, etc.). [6]

This begins to show that due to the increasing complexity as well as the introduction of non-schedulable generation, electric power systems will have to have a new scheme for security assessment. Weather will have an increasingly large effect on the system, and a larger system will be likely to experience more failures. This coupled with the dramatic increase in computing power and a reliance on grid supplied electricity means that new probabilistic methods are not only possible but likely.

For a broad overview of the methods used within power system reliability refer to the works of Billinton and Allen [7].

A. Traditional Power System Security

Power system security involves making sure the system is in an acceptable state, Kirschen [8] provides a good overview to this. In the UK the system operator has only one hour to achieve an acceptable level of security. This involves:

- 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. There are meant trade-offs involved; the goal is to achieve an acceptable level of security at least cost.

Various types of computer simulation can be run to determine the behavior 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.

The list of contingencies to be simulated has traditionally been where each line, transformer, and generator are individually taken out of service [9]. This generates a set known as N-1, where N represents the number of system components; to be N-1 secure is to have a system which remains stable after any N-1 contingency occurs. The UK operates somewhere between N-1 and N-2 (the set of all possible failures on any two components) security; that is, any single component fault and credible double fault should not cause the system to enter an emergency state.

In this way N-x security treats the probability of failure in a simplistic way; it assumes all contingencies to be equally likely. It fails to recognize that intermittent/non-schedulable generators have a quite inaccurate prediction of their output power [10]. It also fails to take into account correlated failure caused by common right of way, common structure or extreme weather conditions.

That said, it remains a very popular scheme and there has been numerous methods to determine a least cost approach to maintaining N-1 security through stability constrained optimal power flow (SCOPF) [11].

To improve the deterministic security assessment there has been significant work to determine the optimal set of contingencies to consider [6] [2] [12]. They often consider external influences such as season or weather to change the working set. As the contingency selection becomes more complex it starts to introduce probability and risk.

B. Risk Based Methods

Risk based (i.e probabilistic) methods are categorized by their use of both probability and consequence. Billinton defines risk as the product of the probability of an event resulting in a security violation and the consequence of that violation [13].

Probabilistic risk assessment is nothing new, it has been used in other industries since the 1960's; and has been studied in power systems since the 1970's [14]. But due to the success of other techniques and the time constraints involved they have been slow to be adopted.

The disadvantage of using the deterministic approach will eventually start to impact financially. In some instances balancing market prices are already increased by the introduction of wind power [5]. For a further explanation on why the once adequate deterministic security assessment methods need to change see [2].

Sobajic et. al. [15] provides a brief overview of four different approaches to the problem of stability assessment:

- Numerical Integration,
- The Second Method of Lyapunov,
- Probabilistic Methods, and
- Pattern Recognition.

The paper then discussed 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 [16] 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 [17] 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 [9]. It also provides a good conceptual representation which shows how risk based security assessment will more accurately reflect the actual level of security. Xiao 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 [18] created a system for aiding control room decisions based on risk.

C. The variability of wind

The introduction of intermittent and non-schedulable generation will have a number of effects. The impact of these effects will depend on the type, installed capacity, climate and geographic distribution of the installed turbines. The inherent intermittentcy of renewable generation means that it cannot displace conventional generation on a "megawatt for megawatt" basis [19], it will however tend to increase balancing market costs [20]. This is not currently a large problem but as penetration increases there will need to be larger reserves or a change in market.

It was the case that wind farms were simply not made to ride-through faults, disconnecting until normal operation resumed. This has a detrimental effect on the system by amplifying the consequence of any fault. They have this feature due to the lack of reactive power control on older SCIG based turbines, in fault conditions they would consume large amounts of reactive power, possibly leading to voltage collapse. The effects of wind power on system dynamics are

Unit group	Unit Size (MW)	Unit Type	Force Outage Rate	MTTF (Hour)	MTTR (Hour)	Scheduled Maint. wks/year
U12	12	Oil/Steam	0.02	2940	60	2
U20	20	Oil/CT	0.10	450	50	2
U50	50	Hydro	0.01	1980	20	2
U76	76	Coal/Steam	0.02	1960	40	3
U100	100	Oil/Steam	0.04	1200	50	3
U155	155	Coal/Steam	0.04	960	40	4
U197	197	Oil/Steam	0.05	950	50	4
U350	350	Coal/Steam	0.08	1150	100	5
U400	400	Nuclear	0.12	1100	150	6

Fig. 1. Generator Reliability Data [23]

covered by a series of papers by Slootweg and Kling including [21]. This shows how newer DFIG cope better with faults and due to advance control electronics can have a stabilizing effect post-fault. A comprehensive review of the effects of integrating wind by Ackermann [22] highlight the danger of cut-off in turbines:

> Wind power reductions due to the cutoff wind speed can, in extreme situations, lead to vary large power deviations. [22]

Work has been done to try and determine the most financially efficient way of trading wind power [10]. This includes a table of expected generation variation between 0.5 and 4 hours after a forecast.

D. Analyzing Security Assessment Methods

Any new security scheme will firstly need to have a set of easy to follow rules that can be determined quickly. it will need to provide a solution that doesn't disadvantage renewable generation while maintaining the same level of security all at least cost.

The security assessment method must also be verifiable, i.e they must be a way to see if the system operator or even the methodology were at fault following an event.

One problem with this is that there isn't really any measure of a level of security so comparing them between different schemes is difficult. That is the aim of this paper.

E. IEEE-RTS

The IEEE-RTS was created to provide a common test-bed for study. It contains a wealth of information from three main papers culminating in [23]. For the purposes of this report a small subset of this will be initially considered:

- *Generator MTTF* (hours)
- *Generator MTTR* (hours)
- *Line fail rate* (outages/year)
- *Line fail duration* (hours)
- *Line transient fail rate* (outages/year)

The data shown comes from the tables in [23] these are included as Fig 1, 2, and 3.

II. Methodology

The method detailed in this project is a mix of completed and proposed work. The results of the completed work is detailed explicitly in the next section. The work is made up of a number of computer programs. These are shown in Fig 4

ID# = Branch identifier.
Inter area branches are indicated by double letter ID.
Circuits on a common tower have hyphenated ID#.
λp = Permanent Outage Rate (outages/year).
Dur = Permanent Outage Duration (Hours).
λt = Transient Outage Rate (outages/year).
Con = Continuous rating.
LTE = Long-time emergency rating (24 hour).
STE = Short-time emergency rating (15 minute).
Tr = Transformer off-nominal ratio.
Transformer branches are indicated by Tr ≠ 0.

ID #	From Bus	To Bus	L miles	λp	Perm- Dur	Tran. λt	R pu	X pu	B pu	Con MVA	LTE MVA	STE MVA	Tr pu
A1	101	102	3	.24	16	0.0	0.003	0.014	0.461	175	193	200	0
A2	101	103	55	.51	10	2.9	0.055	0.211	0.057	175	208	220	0
A3	101	105	22	.33	10	1.2	0.022	0.085	0.023	175	208	220	0
A4	102	104	33	.39	10	1.7	0.033	0.127	0.034	175	208	220	0
A5	102	106	50	.48	10	2.6	0.050	0.192	0.052	175	208	220	0
A6	103	109	31	.38	10	1.6	0.031	0.119	0.032	175	208	220	0
A7	103	124	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
A8	104	109	27	.36	10	1.4	0.027	0.104	0.028	175	208	220	0
A9	105	110	23	.34	10	1.2	0.023	0.088	0.024	175	208	220	0
A10	106	110	16	.33	35	0.0	0.014	0.061	2.459	175	193	200	0
A11	107	108	16	.30	10	0.8	0.016	0.061	0.017	175	208	220	0
AB1	107	203	42	.44	10	2.2	0.042	0.161	0.044	175	208	220	0
A12-1	108	109	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
A13-2	108	110	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
A14	109	111	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
A15	109	112	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
A16	110	111	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
A17	110	112	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
A18	111	113	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
A19	111	114	29	.39	11	0.7	0.005	0.042	0.088	500	600	625	0
A20	112	113	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
A21	112	123	67	.52	11	1.6	0.012	0.097	0.203	500	600	625	0
A22	113	123	60	.49	11	1.5	0.011	0.087	0.182	500	600	625	0
A62	113	215	52	.47	11	1.3	0.010	0.075	0.158	500	600	625	0
A23	114	116	27	.38	11	0.7	0.005	0.059	0.082	500	600	625	0
A24	115	116	12	.33	11	0.3	0.002	0.017	0.036	500	600	625	0
A25-1	115	121	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
A25-2	115	121	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
A26	115	124	36	.41	11	0.9	0.007	0.052	0.109	500	600	625	0
A27	116	117	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A28	116	119	16	.34	11	0.4	0.003	0.023	0.049	500	600	625	0
A29	117	118	10	.32	11	0.2	0.002	0.014	0.030	500	600	625	0
A30	117	122	73	.54	11	1.8	0.014	0.105	0.221	500	600	625	0
A31-1	118	121	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A31-2	118	121	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A32-1	119	120	27.5	.38	11	0.7	0.005	0.040	0.083	500	600	625	0
A32-2	119	120	27.5	.38	11	0.7	0.005	0.040	0.083	500	600	625	0
A33-1	120	123	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
A33-2	120	123	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
A34	121	122	47	.45	11	1.2	0.009	0.068	0.142	500	600	625	0
AB3	123	217	51	.46	11	1.3	0.010	0.074	0.155	500	600	625	0
B1	201	202	3	.24	16	0.0	0.003	0.014	0.461	175	193	200	0
B2	201	203	55	.51	10	2.9	0.055	0.211	0.057	175	208	220	0
B3	201	205	22	.33	10	1.2	0.022	0.085	0.023	175	208	220	0
B4	202	204	33	.39	10	1.7	0.033	0.127	0.034	175	208	220	0
B5	202	206	50	.48	10	2.6	0.050	0.192	0.052	175	208	220	0
B6	203	209	31	.38	10	1.6	0.031	0.119	0.032	175	208	220	0
B7	203	224	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
B8	204	209	27	.36	10	1.4	0.027	0.104	0.028	175	208	220	0
B9	205	210	23	.34	10	1.2	0.023	0.088	0.024	175	208	220	0
B10	206	210	16	.33	35	0.0	0.014	0.061	2.459	175	193	200	0
B11	207	208	16	.30	10	0.8	0.016	0.061	0.017	175	208	220	0
B12-1	208	209	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
B13-2	208	210	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
B14	209	211	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
B15	209	212	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
B16	210	211	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
B17	210	212	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
B18	211	213	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
B19	211	214	29	.39	11	0.7	0.005	0.042	0.088	500	600	625	0
B20	212	213	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
B21	212	223	67	.52	11	1.6	0.012	0.097	0.203	500	600	625	0
B22	213	223	60	.49	11	1.5	0.011	0.087	0.182	500	600	625	0
B23	214	216	27	.38	11	0.7	0.005	0.059	0.082	500	600	625	0
B24	215	216	12	.33	11	0.3	0.002	0.017	0.036	500	600	625	0
B25-1	215	221	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
B25-2	215	221	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
B26	215	224	36	.41	11	0.9	0.007	0.052	0.109	500	600	625	0
B27	216	217	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
B28	216	219	16	.34	11	0.4	0.003	0.023	0.049	500	600	625	0
B29	217	218	10	.32	11	0.2	0.002	0.014	0.030	500	600	625	0
B30	217	222	73	.54	11	1.8	0.014	0.105	0.221	500	600	625	0
B31-1	218	221	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
B31-2	218	221	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
B32-1	219	220	27.5	.38	11	0.7	0.005	0.040	0.083	500	600	625	0
B32-2	219	220	27.5	.38	11	0.7	0.005	0.040	0.083	500	600	625	0
B33-1	220	223	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
B33-2	220	223	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
B34	221	222	47	.45	11	1.2	0.009	0.068	0.142	500	600	625	0

Fig. 2. Line Reliability Data [23]

and described below. Basically it creates a set of initial states, sample each of them many times and simulate the samples; these results are then analyzed.

1) Initial State Generator: The initial state generator produces two parts, the load flow and the list of components on outage. In other words it creates a system in a working state as the system operator expects it to be. The load flow is made from the output at each generator and the demand at each busbar.

This information can either be created from a representative sample of historic data; or, as in this case, from the data files. The demand profile in the IEEE-RTS can be used to produce one half of the load flow with the other coming from basic fuel cost data. The fuel cost can determine the generator output through some sort of optimal power flow program. For renewable generators a statistical analysis of the wind resource for each site could produce a set of samples.

ID #	From Bus	To Bus	L miles	-Perm- Δp	Dur	Tran. Δt	R pu	X pu	B pu	Con MVA	LTE MVA	STE MVA	Tr pu
C1	301	302	3	.24	16	0.0	0.003	0.014	0.461	175	193	200	0
C2	301	303	55	.51	10	2.9	0.055	0.211	0.057	175	208	220	0
C3	301	305	22	.33	10	1.2	0.022	0.085	0.023	175	208	220	0
C4	302	304	33	.39	10	1.7	0.033	0.127	0.034	175	208	220	0
C5	302	306	50	.48	10	2.6	0.050	0.192	0.052	175	208	220	0
C6	303	309	31	.38	10	1.6	0.031	0.119	0.032	175	208	220	0
C7	303	324	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
C8	304	309	27	.36	10	1.4	0.027	0.104	0.028	175	208	220	0
C9	305	310	23	.34	10	1.2	0.023	0.088	0.024	175	208	220	0
C10	306	310	16	.33	35	0.0	0.014	0.061	2.459	175	193	200	0
C11	307	308	16	.30	10	0.8	0.016	0.061	0.017	175	208	220	0
C12-1	308	309	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
C13-2	308	310	43	.44	10	2.3	0.043	0.165	0.045	175	208	220	0
C14	309	311	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
C15	309	312	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.03
C16	310	311	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
C17	310	312	0	.02	768	0.0	0.002	0.084	0	400	510	600	1.015
C18	311	313	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
C19	311	314	29	.39	11	0.7	0.005	0.042	0.088	500	600	625	0
C20	312	313	33	.40	11	0.8	0.006	0.048	0.100	500	600	625	0
C21	312	323	67	.52	11	1.6	0.012	0.097	0.203	500	600	625	0
C22	313	323	60	.49	11	1.5	0.011	0.087	0.182	500	600	625	0
C23	314	316	27	.36	11	0.7	0.005	0.059	0.082	500	600	625	0
C24	315	316	12	.33	11	0.3	0.002	0.017	0.036	500	600	625	0
C25-1	315	321	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
C25-2	315	321	34	.41	11	0.8	0.006	0.049	0.103	500	600	625	0
C26	315	324	36	.41	11	0.9	0.007	0.052	0.109	500	600	625	0
C27	316	317	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
C28	316	319	16	.34	11	0.4	0.003	0.023	0.049	500	600	625	0
C29	317	318	10	.32	11	0.2	0.002	0.014	0.030	500	600	625	0
C30	317	322	73	.54	11	1.8	0.014	0.105	0.221	500	600	625	0
C31-1	318	321	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
C31-2	318	321	18	.35	11	0.4	0.003	0.026	0.055	500	600	625	0
C32-1	319	320	27.5	.36	11	0.7	0.005	0.040	0.083	500	600	625	0
C32-2	319	320	27.5	.36	11	0.7	0.005	0.040	0.083	500	600	625	0
C33-1	320	323	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
C33-2	320	323	15	.34	11	0.4	0.003	0.022	0.046	500	600	625	0
C34	321	322	47	.45	11	1.2	0.009	0.068	0.142	500	600	625	0
CA-1	325	121	67	.52	11	1.6	0.012	0.097	0.203	500	600	625	0
CB-1	318	223	72	.53	11	1.8	0.013	0.104	0.218	500	600	625	0
C35	323	325	0	.02	768	0.0	0.000	0.009	0	722	893	893	1.00

Fig. 3. Line Reliability Data cont. [23]

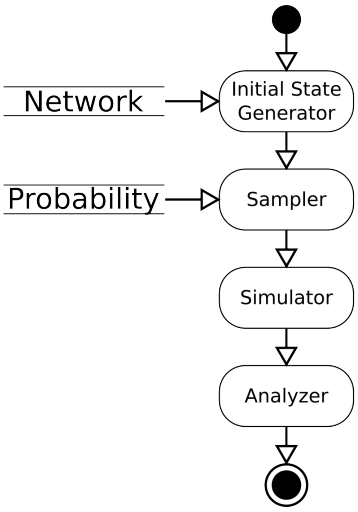

Fig. 4. Example of included graphics

$$P_o = \frac{MTTF}{(MTTF + MTTR)} \tag{1}$$

where;

- $MTTF$ is the mean time to fail in hours
- $MTTR$ is the mean time to repair in hours

The components on outage can be obtained from the MTTF and MTTR through Markov Models. A simple probability of outage can be calculated as in equation 1 using the data from Fig 1.

Both the MTTF and MTTR can be sampled (using equation 2 to produce a TTF_0 and TTR_0. A random number selected between these values not only shows where the component is in service but when it will change state.

$$T_0 = -xlog(1 - U[0,1]) \tag{2}$$

where;

- x is the mean time
- $U[0,1]$ is a uniform random number in the range 0 to 1

2) Sampler: The sampler takes one initial state, with some probability data to produce a final sample. Each time it is run it can produce a different sample based on the likelihood of events. The three additional outputs that are added to the initial state are:

- *Component Failures*
- *Variation in Generation*
- *Variation in Demand*

Failures are again consider here to distinguish between a component that was previously out and has little effect on the system, with a component that fails during simulation.

The probability information available from the IEEE-RTS can be used on any initial system to come up with a probability of any component being in a certain state. For lines the probability is equation 3.

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

where;

- λ is the failure rate from Fig 2
- t is the time period. 0.5h in this case.

The variation in renewable generator power is not consider here but should come from an analysis of the variation in wind response over the time-frame simulated; in the UK this is half-hour blocks.

Many of the simulations produce the same result. To reduce the computational burden of simulation these can be consolidated into a single simulation.

3) Simulator: A dynamic simulator such as PSAT can be used to take each sample and say whether the resulting simulation leaves the system in a suitable state or not. A simple definition of a suitable state is that the system remains stable and not outside of limits. A more advanced definition could cover load not served and power quality.

4) Analyzer: This program consolidates the results of the simulator and other programs into readable results. These results and their formation are described next.

Each initial state can have associated with it a probability of failure by looking at the number of samples that failed. An ideal security assessment method would signal a failure if the probability of failure was above some threshold and a success if it was below. By comparing other system security schemes to this ideal we can say how many times it is in error. To extend this idea we can look not only at the number of initial states were reported incorrectly but also how badly wrong they were. The measure of how badly it was wrong is simply the difference between the threshold and the probability of failure in each initial state where it was wrong.

III. Results

The work done involved creating initial states, sampling those states and analyzing the data produced. This is detailed below.

TABLE I
SUBSET OF SAMPLED DATA

Occurrence	No. Events	Trans	Fail	Simulation
784349	0			
2220	1	G01		
2203	1	G38		
2190	1	G71		
2162	1	G04		
2149	1	G67		
...	...	...	...	...
23	1		C30	
23	1		B34	
23	1		B32-2	
22	1	A33-1		
22	1		B25-2	
...	...	...	...	...

The process of creating the initial state involved seeing which components (generators and lines) were out of service. For generators this can be done directly from equation 2, lines require changing the failure rate into a mean time beforehand.

The sampler randomly picks one initial state and runs many samples from it. The samples include whether a generator or line fails during the half-hour simulation. Lines can fail either as a transient or permanent failure. For each generator in the system a Markov Model can determine both the initial state and time remaining in that state using equation 2. If the time remaining is less than the simulation time then the generator will fault (or be repaired, but repaired generators are not turned back on during blocks). Equation 3 can create the probability of each line failing during the next half-hour, if a uniformly distributed random number between 1 and 0 is less than this then the line is set to fail.

The sampler was run over many hours to produce a set of around 900,000 samples. These were consolidated to remove duplicated entires. A small subset of this file is shown in Table I. In here it can be seen that around 780,000 samples had no failure at all and that there were about 2000 samples where component G01 failed.

The next stage was to group the results into the number of failures, i.e. create groups for each N-x. This is shown in Table II. 87% of samples has no failures at all; 12% had one component failing. These numbers may seem high; this is due to the IEEE-RTS treating each generator by its separate units; one busbar may have many generators attached. The last column in the table shows the probability of the class of failures given that one has occurred. Hence, there is a 93% chance that a failure that occured will be N-1, this yields some surprising results: for this system 6.5% of all failures are N-2 and 0.3% actually had more than two components failing simultaneously. It can be seen from the graph in Fig 5 that the decay is exponential.

TABLE II
FAILURES OF TYPES N-X

Type	Occurrence	Probability per Simulation	Probability per Failure
N-0	784349	0.86764	-
N-1	111450	0.12329	0.93146
N-2	7808	0.00864	0.06526
N-3	382	0.00042	0.00319
N-4	10	0.00001	0.00008
N-5	1	0.00000	0.00001
N-6	0	0.00000	0.00000

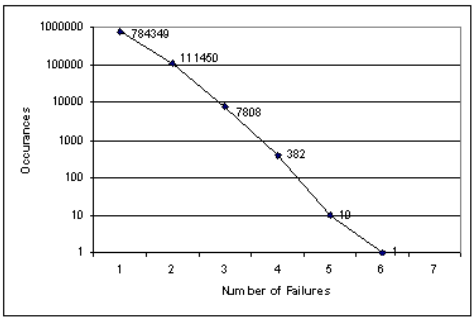

Fig. 5. Likelihood of Failure

IV. CONCLUSION

The results show that 87% of samples had no failures at all. Which, if operating conditions remain the same, gives an expected time to fail of once every 8 hours. It should be noted that this time to fail figure is quite high. This is due to the generators being treated as individual units rather than being aggregated by busbar. 93% of failures were on one components which means almost 7% of the time when a failure occurred it was on more than one component. This highlights just how important it is to go beyond N-1 security.

The probability of getting an N-2 was roughly an order of magnitude less than N-1. This seemed to hold true for the other N-x cases. There was a small number of simulations where multiple generating units failed; this is likely to affect the system very badly. It has been shown that the cost of losing the entire system is many times greater than multiple losses of individual parts.

It highlights the need for a new security assessment scheme that goes beyond a small deterministic set of test cases, particularly in large systems or systems with a high percentage of renewable generation.

ACKNOWLEDGMENT

This work was sponsored by The Supergen Flexnet Consortium.

REFERENCES

[1] NERC, "Nerc planning standards," *The North American Reliability Council*, 1997.

[2] 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.

[3] 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

[4] BWEA, "Annual review 2006," BWEA, Tech. Rep., 2006. [Online]. Available: http://www.bwea.com/pdf/BWEA_annual_review_2006.pdf

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

[6] 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.

[7] 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

[8] 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$_all.jsp?arnumber = 1106706$

[9] 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.

[10] G. Bathurst, J. Weatherill, and G. Strbac, "Trading wind generation in short term energy markets," *Power Systems, IEEE Transactions on*, vol. 17, no. 3, pp. 782–789, 2002.

[11] X. Zhang, "Hight speed stability constrained optimal power flow for the electricity balancing market," Ph.D. dissertation, University of Bath, 2007.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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

[18] 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.

[19] G. Strbac, A. Shakoor, M. Black, D. Pudjianto, and T. Bopp, "Impact of wind generation on the operation and development of the uk electricity systems," *Electric Power Systems Research*, vol. 77, no. 9, pp. 1214 – 1227, 2007, distributed Generation. [Online]. Available: http://www.sciencedirect.com/science/article/B6V30-4M4KK9Y-1/2/7309abb9d92fb88781c766d8476e618a

[20] R. Ford and D. Milborrow, "Integrating renewables," BWEA, Tech. Rep., Feb 2005. [Online]. Available: http://www.bwea.com/pdf/RAEIntegrationfinal.pdf

[21] J. Slootweg and W. Kling, "Impacts of distributed generation on power system transient stability," in *Power Engineering Society Summer Meeting, 2002 IEEE*, vol. 2, 25-25 July 2002, pp. 862–867vol.2.

[22] T. Ackermann, *Wind in power systems*. John Wiley & Sons (21 Jan 2005), 2005. [Online]. Available: http://www.amazon.co.uk/exec/obidos/ASIN/0470855088/interactiveda51-21

[23] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, and C. Singh, "The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," *Power Systems, IEEE Transactions on*, vol. 14, no. 3, pp. 1010–1020, Aug 1999.