High Renewable Energy Penetration and Power System Security: New Challenges and Opportunities

Michael Negnevitsky

EIER 2022
13 January 2022
Hanoi

Centre for Renewable Energy and Power Systems
UNIVERSITY OF TASMANIA

Prof Michael Negnevitsky

Chair in Power Engineering and Computational Intelligence
Director of the Centre for Renewable Energy and Power Systems
School of Engineering
University of Tasmania
Private Bag 65 Hobart
Tasmania, 7001 Australia

Contents

- Concept of power system security.
- Operating reserves.
- Inertial and primary frequency response.
- Impact of renewable energy generation.
- Risk-based security assessment.
- Conclusions.

Introduction

- The word “security” in the context of a power system implies its security against a complete collapse, or a blackout. Secure operation involves practices aimed to keep the system operating normally when contingencies occur.
- An increasing penetration of intermittent renewable energy generation introduces additional uncertainties in power systems.

Power system security (cont.)

- Power systems are designed and operated to withstand contingencies selected on the basis of their probabilities.
- In practice, these contingencies are usually defined as the loss of any single major component in a power system.
- We cannot stop contingencies from happening, and we cannot predict when they will occur. But we can model potential contingencies and analyse their consequences.

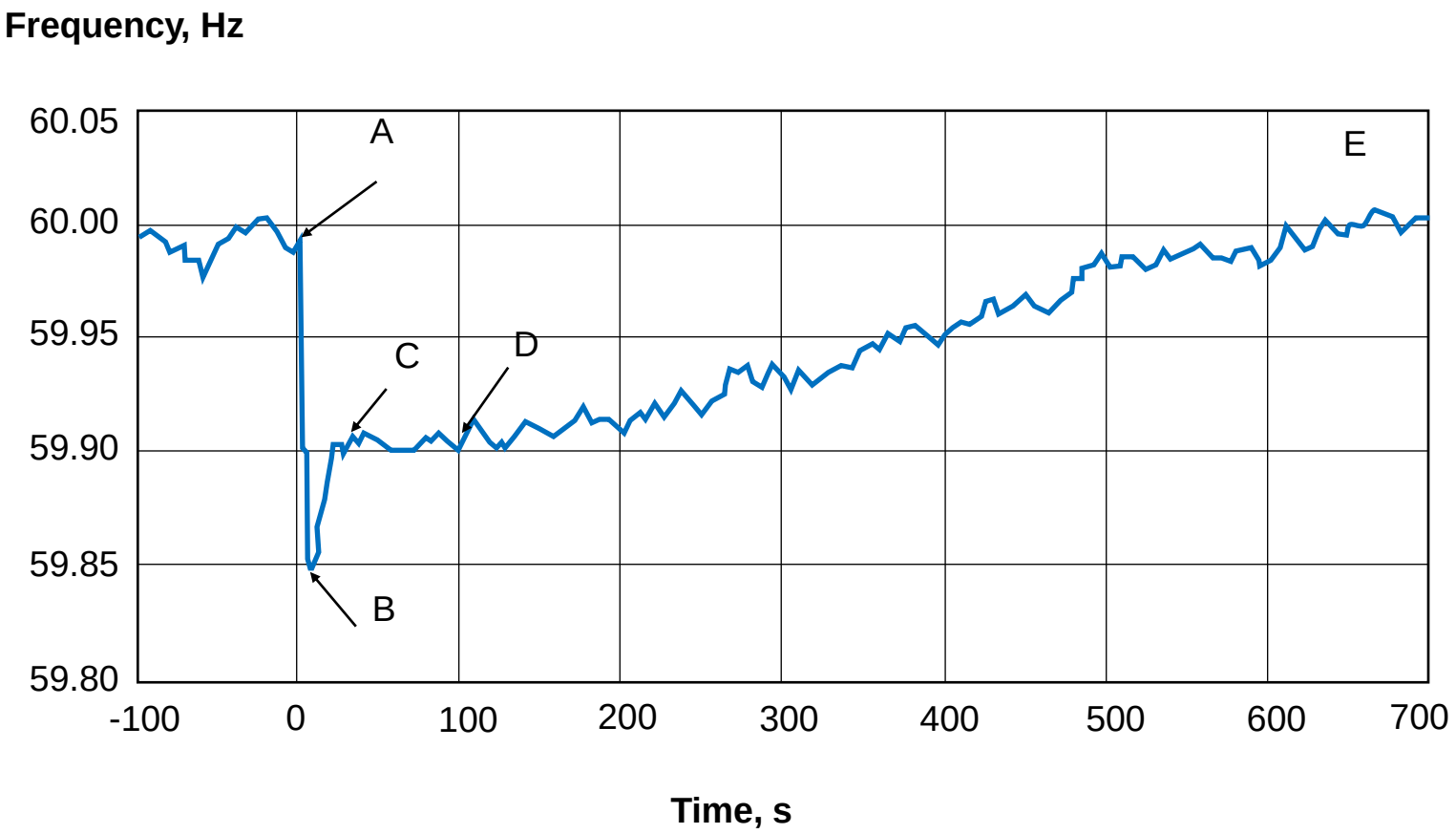
Operating reserves

- To ensure the required level of security, a power system must have sufficient reserves.
- These reserves are needed to balance short-term variations in supply and demand, mitigate the effects of load forecasting errors, handle peak demand, and manage fluctuations in renewable energy generation.
- But most of all, reserves are needed to withstand contingencies.

Operating reserves (cont.)

- Power system equipment is subject to random failures, and thus additional generation capacity is needed so that it can be called upon when a large generator or a heavily loaded transmission line is suddenly taken out of service. This additional capacity is referred to as *operating reserve*.

Contingency event and a typical system response



Inertial response

- At the very instant of the generation loss, synchronous generators that are still connected to the grid release kinetic energy stored in their rotating masses (turbines, shafts and rotors), and thereby slow down the frequency decline.
- This type of response is called ***inertial* response**. Large fast rotating generators have larger inertial response than smaller or slowly rotating machines. The system inertia, or the cumulative inertial response of all rotating machines, determines the initial slope of the frequency decline.

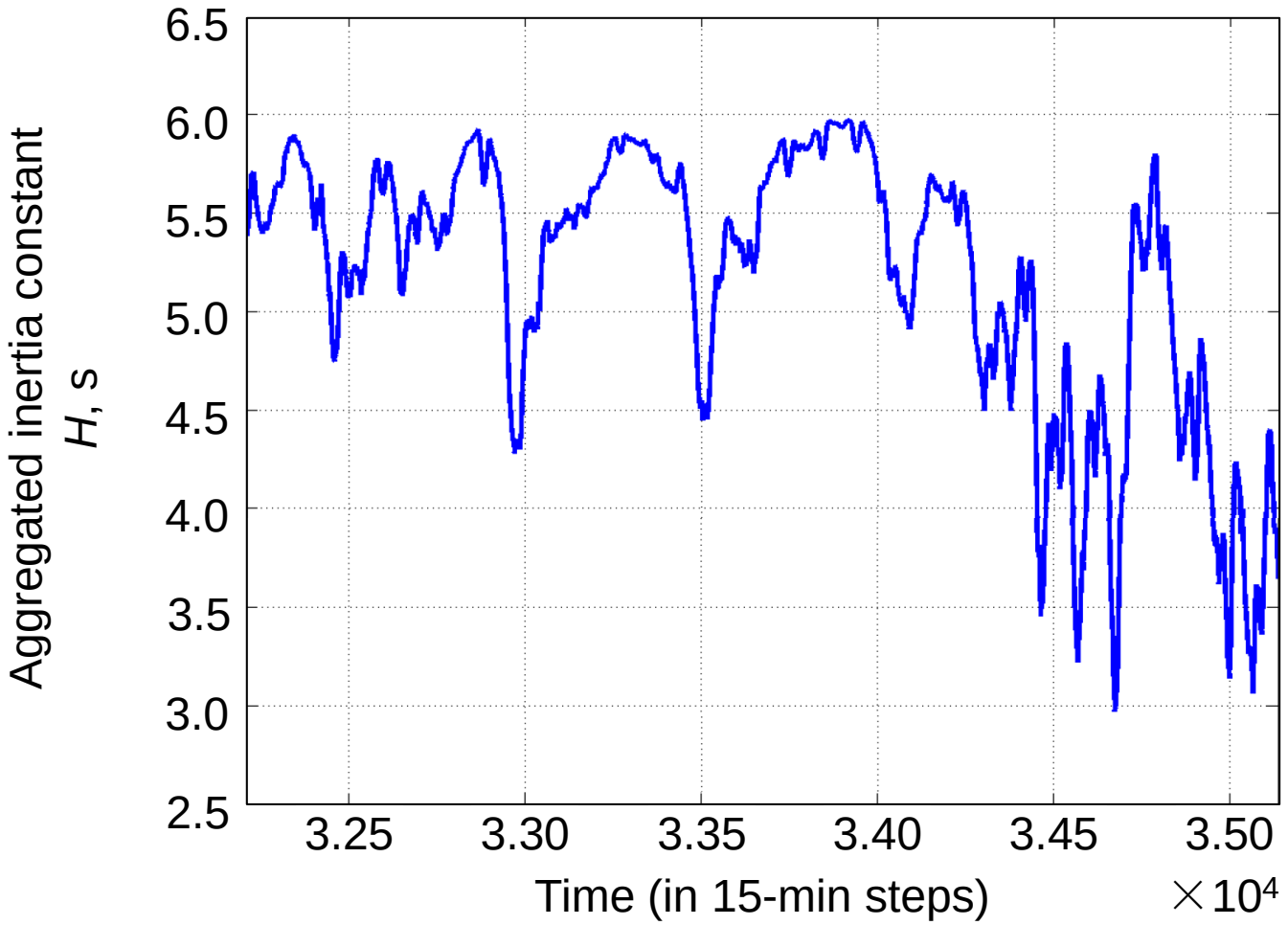
Impact of Renewable Energy Generation

- An increasing penetration of intermittent renewable energy generation introduces additional uncertainties in power systems.
- However, the impact of variable generation on the system security is often exaggerated. For example, in the Ireland and Northern Ireland power system, the system stability degrades only when non-synchronous variable generation exceeds 50% of demand.
- No significant mitigation measures are required until the wind and solar penetration reaches 20%.

The main challenge facing a power system with high penetration of renewables is the displacement of conventional synchronous generation by non-synchronous generation.

Impact of Renewable Energy Generation (cont.)

- Kinetic energy stored in the rotating masses of synchronous generators provides the system rotational inertia.
- Wind power generators are decoupled from the grid by electronic converters – they do not provide inertia to the system. This reduces the total system inertia.
- The system becomes more vulnerable to contingencies – even contingencies that previously were considered “safe” can now lead to frequency violations and the system’s instability.



Aggregated rotational inertia in the German power system. Conventional generators provide inertia of 6 s and wind and PV generators do not contribute any inertia.

Inertia constant

- The inertia constant is expressed in seconds. It indicates the duration that the generator can supply its rated power to the system using only its kinetic energy.
- For example, the inertia constant of 6 s means that the generator can supply its rated power to the system for 6 s using only energy stored in its rotating masses.

Case study

- Six 200 MVA and ten 100 MVA synchronous generators are supplying a total load of 2000 MW. The inertia constant of each 200 MVA unit is 5.0 s on the 200 MVA base, and the inertia constant of each 100 MVA unit is 4.0 s.
- Determine the frequency deviation following a sudden loss of one of the 200 MVA units.
- Examine the frequency dynamics of the system when five 100 MVA synchronous generators are displaced by non-synchronous renewable generation.

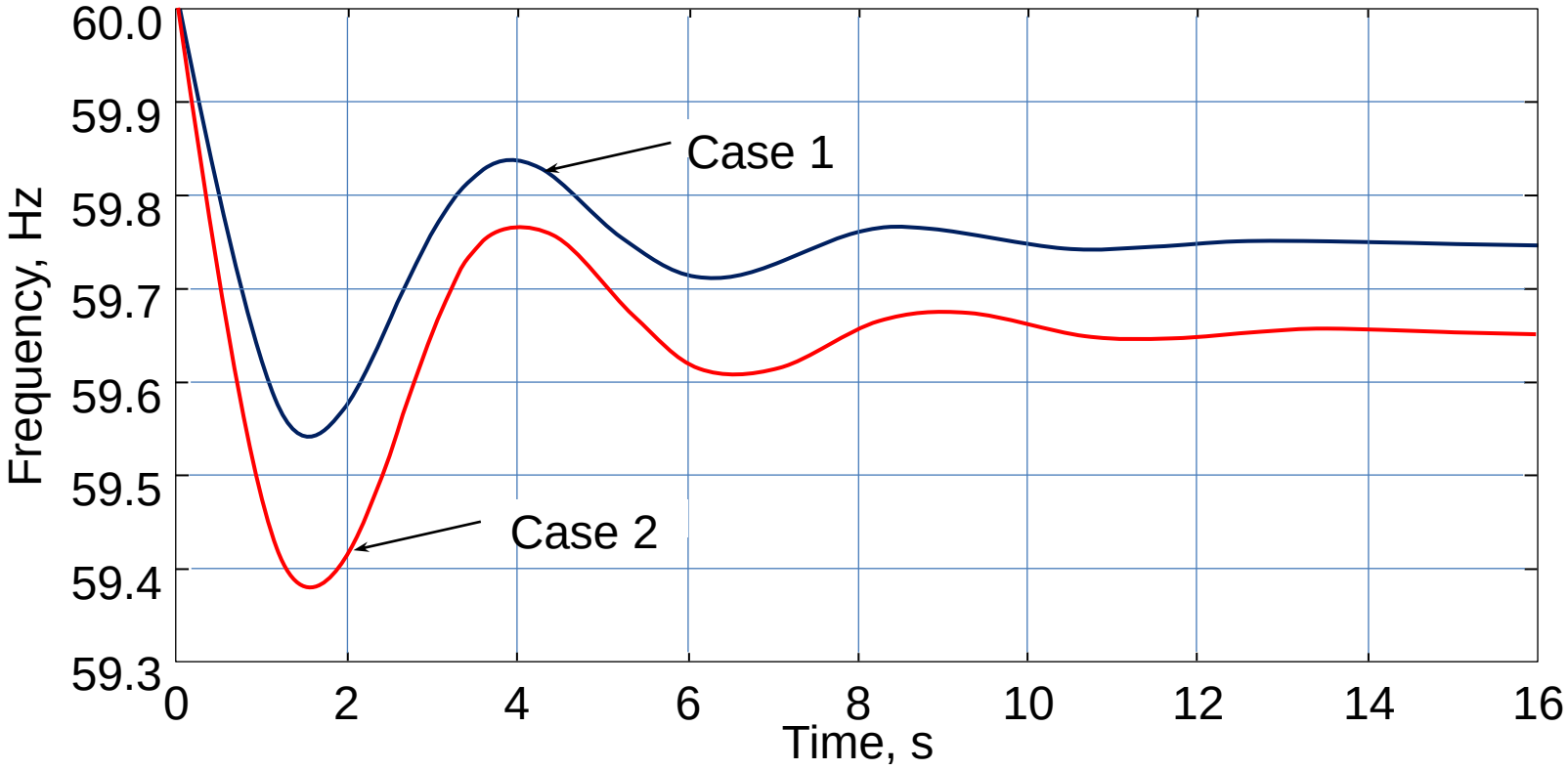
The total system inertia constant following the contingency:

$$H = \frac{5000 + 4000}{1000} = 9\ s$$

The system frequency dynamics when five 100 MVA synchronous generators are displaced by non-synchronous power generators:

$$H = \frac{5000 + 2000}{1000} = 7\ s$$

Frequency response of the power system



Frequency in the “lighter” case declines much faster, although in both cases, the system has sufficient rotating reserves to cover for the loss of the largest generator.

Risk-based Security Assessment

- Traditionally security assessment is performed based on deterministic criteria. The *N*-1 security criterion requires a power system to withstand an outage of any single system component without violating any system operating limits.
- It has satisfied the needs of the power industry for decades. However, the deterministic approach to security may not be adequate in modern power systems with market driven dispatch and high penetration of renewable energy and distributed generation.

Risk-based Security Assessment

- Traditionally security assessment is performed based on deterministic criteria. The *N*-1 security criterion requires a power system to withstand an outage of any single system component without violating any system operating limits.
- It has satisfied the needs of the power industry for decades. However, the deterministic approach to security may not be adequate in modern power systems with market driven dispatch and high penetration of renewable energy and distributed generation .

Risk-based Security Assessment (cont.)

- Deterministic security criteria define a set of "credible" contingencies that the system should be able to withstand.
- However, that the deterministic contingency analysis does take the probabilities of contingencies into account – the selection of "credible" contingencies implicitly implies that these contingencies are more likely to occur in reality.

Risk-based security definition

- Security can be defined as the risk in the system's ability to withstand random contingencies without interruption to customer service. The higher the risk the lower the security.
- Although risk cannot be eliminated fully due to unexpected faults and probabilistic behaviour of a power system, it can be assessed and managed within an acceptable level in power system planning, design and operation.

Risk-based security definition

- Risk-based security analysis is concerned with voltage violations, overloads and frequency response adequacy.
- Frequency response adequacy is defined as the capability of frequency response resources to prevent frequency from dropping below a certain limit.
- We need to assess the primary frequency response because of the risk of under-frequency load shedding, particularly in systems with low inertia.

Risk-based security assessment

- In risk-based security assessment, we do not use a predefined list of contingencies, but generate contingencies at random based on their probabilities.
- Then, we assess the consequences of these contingencies to determine whether loads are disconnected following voltage violations, overloads and significant imbalance between load and generation. This allows us to measure the impact of random contingencies in terms of loads not served.

The value of risk

$$Risk = \sum_{n=1}^{N} \sum_{m=1}^{M} p(S_n) \cdot p(C_{nm}) \cdot Sev(C_{nm})$$

where *Risk* is the risk index,

$p(S_n)$ is the probability of the pre-contingency operating state S_n,

$p(C_{nm})$ is the probability of contingency C_m occurring in the state S_n,

$Sev(C_{nm})$ is the severity of the contingency C_m in the state S_n,

N is the total number of pre-contingency operation states, and M is the total number of contingencies considered in each state.

Conclusions

- The main challenge facing a power system with high penetration of renewables is the displacement of conventional synchronous generation by non-synchronous generation.
- The deterministic approach to security may not be adequate in modern power systems with market driven dispatch and high penetration of renewable energy and distributed generation.
- In risk-based security assessment, we generate contingencies at random, based on their probabilities.