Cyber Security of Power System Control Systems

The widespread adoption of components with communication capabilities and internet-connectivity in power systems have increased the vulnerability of those power systems to damaging and potentially dangerous cyber-attacks. New methods are urgently required to rapidly and accurately detect attacks and protect control systems.

Competitive advantage

- Advanced, detailed modelling of the dynamics of power systems across the essential timescales required
- Expertise in the application of nonlinear systems theory for the detection of attacks on power system control systems
- An experienced interdisciplinary research team with a significant collaborative track record in the fusion of electrical power engineering and advanced control techniques
- Broad applicability to conventional central grids as well as grid-connected and islanded microgrids

More Information

Dr Hendra I Nurdin, Professor John Fletcher

School of Electrical Engineering and Telecommunications

T: +61 (0) 2 9385 7556
E: h.nurdin@unsw.edu.au, john.fletcher@unsw.edu.au

UNSW Knowledge Exchange

knowledge.exchange@unsw.edu.au

www.capabilities.unsw.edu.au

+61 (2) 9385 5008

Impact

- A control theory approach to assessing cyber security threats reduces uncertainty

Capabilities and facilities

- State-of-the-art real-time digital simulation facilities for hardware-in-the-loop testing of power-related communication equipment
- State-of-the-art high-voltage and microgrid facilities for experimental verification
- Dedicated communications laboratories

Our partners

- Network operators
- Equipment manufacturers