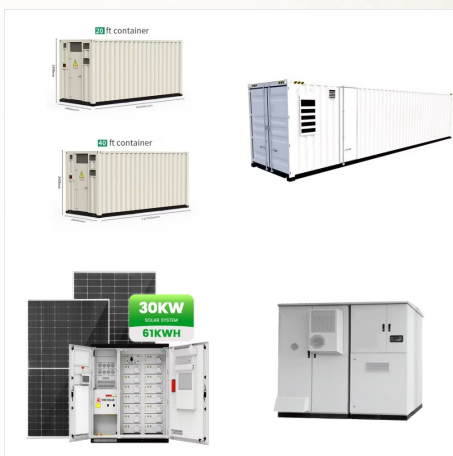


The development of a trustworthy smart grid requires a deeper understanding of potential impacts resulting from successful cyber attacks. Estimating feasible attack impact requires an evaluation of the grid's dependency on its cyber infrastructure and its ability to tolerate potential failures. A further exploration of the cyber-physical relationships within the smart grid and a specific



Cyber-physical security issues: Having a developed and smart control system in the power network can considerably improve the stability of the whole system against possible fluctuations. So far, in smart grids, attention has been paid to the sectors of power generation and energy consumption by consumers.



This paper presents the state-of-art communication technologies that can meet the communication requirements of the various SG-CPS applications and identifies the research gaps in the various domains of the SG- CPS that can be of immense benefit to the research community. The recent developments in embedded system design and communication technologies ???

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



The evolution of power systems into Cyber Physical Power Systems (CPPS), characterized by the integration of information and communication technologies with traditional electrical infrastructure, has resulted in new opportunities and challenges.



3.1 Cyber Attacks and Corresponding Mitigation Strategies. Vulnerability analysis of cyber-physical systems subject to cyber attacks has recently become a growing concern. A typical technique is to analyse the effects of particular attacks against specific systems [1] deception attacks against control systems are defined where deception attacks correspond ???

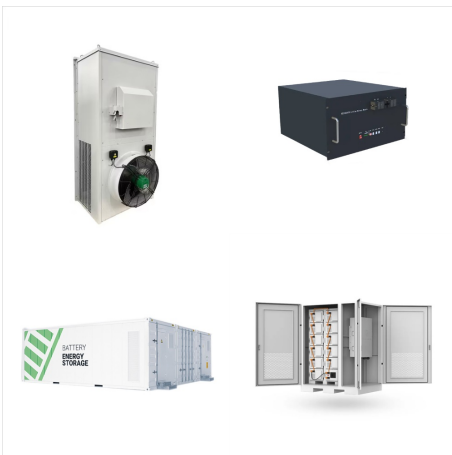


Cyber-Physical System Security of the Power Grid  
Chen-Ching Liu American Electric Power Professor  
Director, Center for Power and Energy Virginia Tech  
Research Professor Washington State University  
Sponsored by U.S. National Science Foundation  
and Science Foundation Ireland, Murdock  
Charitable Trust, ESIC Washington State University,  
State of

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



The smart electricity grids have been evolving to a more complex cyber-physical ecosystem of infrastructures with integrated communication networks, new carbon-free sources of power generation



To achieve this goal, this paper covers: (1) a survey of the state-of-the-art smart grid technologies, (2) power industry practices and standards, (3) solutions that address cyber security issues, (4) a review of existing CPS testbeds for cyber security research, and (5) unsolved cyber security problems. Power grid cyber security research has

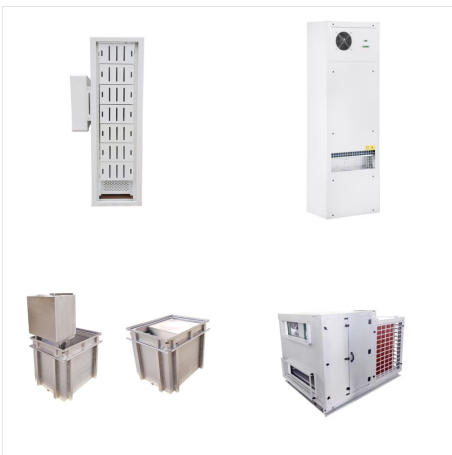


The significance of cyber infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber attacks is highlighted and a layered approach is introduced to evaluating risk based on the security of both the physical power applications and the supporting cyber infrastructure. The development of a trustworthy smart grid requires a deeper ???

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



The research on cyber-physical security of the smart grid advances on a frontier of CPS, striving at the intersection of physical security of power and energy systems and the cybersecurity of information, computation, and communication systems . Incorporation of the strengths of physical and cybersecurity is an essential requirement for the



and the need for security at multiple levels of the cyber-physical power system, namely, information security, information and communication technologies (ICT) infrastructure security, and applicationlevel security. It - identifies cyber security research issues beyond the tradition information technology (IT) security issues.



and the need for security at multiple levels of the cyber-physical power system, namely, information security, rmation and communication technologies info (ICT) infrastructure security, and applicationlevel security. It - identifies cyber security research issues beyond the tradition information technology (IT) security issues.



# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



1 INTRODUCTION. In 2006, the United States (US) National Science Foundation (NSF) first proposed the concept of Cyber-Physical Systems (CPS). CPS integrates the computing system, communication network and ???



The smart electricity grids have been evolving to a more complex cyber-physical ecosystem of infrastructures with integrated communication networks, new carbon-free sources of power generation



This survey discusses such major directions and recent advancements from a lens of different detection techniques, equipment protection plans, and mitigation strategies to enhance the energy delivery infrastructure resilience and operational endurance against cyber attacks. The smart electricity grids have been evolving to a more complex cyber-physical ecosystem of ???

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



A. Cyber-physical systems The term cyber-physical systems (CPS) emerged around 2006, when it was coined at the National Science Foundation (NSF) in the United States [1], with the "cyber" part of the name resulting from the term "cybernetics", introduced as metaphor apt for control systems [11].  
(a) The three main functional components

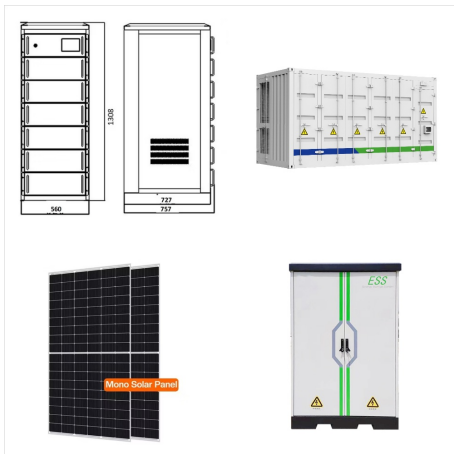


If these measurements are used as input to the state estimation algorithm, the algorithm may produce incorrect internal state estimates leading to severe consequences, such as blackouts, power system disruptions, islanding etc. FDI attacks can be deployed to the different layers of the smart grid, such as physical layer, communication layer



1 INTRODUCTION. In 2006, the United States (US) National Science Foundation (NSF) first proposed the concept of Cyber-Physical Systems (CPS). CPS integrates the computing system, communication network and physical environment through computing, communication and control technologies to form a multi-dimensional and heterogeneous ???

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



In today's standards, the power grid is characterized as a cyber-physical system (CPS) shown in Figure 2, which contains physical, sensor/actuator, network, control, and information layers. Manipulation of each layer is possible but does not necessarily mean an intrusion detection component or system needs to be applied in all layers. Infor-

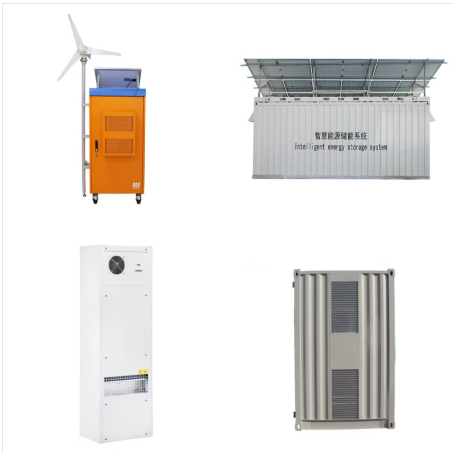


Cyber-physical system Cyber security Intrusion detection CPS testbed Smart grid ABSTRACT The integration of computing and communication capabilities with the power grid has led to numerous vulnerabilities in the cyber-physical system (CPS). This cyber security threat can significantly impact the physical infrastructure, economy, and society.



Keywords: critical infrastructure, cyber-physical security, cybersecurity, power grid, power system communication. 1. Introduction. Historically, power grids have grown from simple, localized grids to large, physically wide-spread grids, often spanning multiple nations or even whole continents . Despite its importance to modern society, the

# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



The introduction of control and automation into the grid has several benefits as discussed in the previous sections. However, the introduction of Smart Grid Cyber-Physical System (SG-CPS) also has several challenges that are yet to be resolved. Some of the most significant challenges of a cyber-physical power system are as follows: 1.



Journal Article: Cyber-Physical System Security of a Power Grid: State-of-the-Art In this paper, a survey of the state-of-the-art is conducted on the cyber security of the power grid concerning issues of: the structure of CPSs in a smart grid; cyber vulnerability assessment; cyber protection systems; and testbeds of a CPS. At Washington



The Cyber-Physical Power System (CPPS) modernizes the traditional electric power grid and is referred to as the next-generation power system [1], [2]. Future grids can be defined as an electric system that integrates two-way, cyber-secure communication technologies, and computational intelligence across electricity generation, transmission, distribution, ???



# CYBER-PHYSICAL SYSTEM SECURITY OF A POWER GRID STATE-OF-THE-ART



Characteristics and focus: the bulk of the works on CPS security is focused on power grids, while somehow surprisingly, we have not found any work on the cyber-physical security of medical CPS, and only a small part of selected papers is within the application field of secure control of (unmanned) ground vehicles and aerial systems, and of



A cyber-physical testbed is critical for the study of cyber-physical security of power systems. For reason of security by power companies, real measurements (e.g., voltages, currents and binary status) and ICT data (e.g., communication protocols, ???