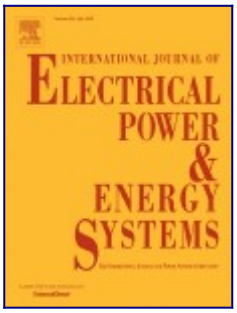
International Journal of Electrical Power & Energy Systems

Volume 99, July 2018, Pages 45-56



Review

Cyber security of a power grid: State-of-the-art

Author links open overlay panelChih-Che Sun [a], Adam Hahn [a], Chen-Ching Liu [a b]

https://doi.org/10.1016/j.ijepes.2017.12.020Get rights and content

Highlights

- •

  A review of cyber systems in a smart grid is provided with a list of the communication standards.

- •

  Requirements for cyber security and industry practice are discussed.

- •

  The state-of-the-art cyber protection and cyber-physical system testbeds are summarized.

- •

The proposed methodology for detection of coordinated cyber attacks is demonstrated.

- •

  Unsolved cyber vulnerabilities that require future research are described.

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. In traditional IT environments, there are already abundant attack cases demonstrating that unauthorized users have the capability to access and manipulate sensitive data from a protected network domain. Electric power grids have also heavily adopted information technology (IT) to perform real-time control, monitoring, and maintenance tasks. In 2015, a sophisticated cyber attack targeted Ukrainian’s power grid causing wide area power outages. It highlights the importance of investment on cyber security against intruders. This paper provides a state-of-the-art survey of the most relevant cyber security studies in power systems. It reviews research that demonstrates cyber security risks and constructs solutions to enhance the security of a power grid. 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 been conducted at Washington State University (WSU) with a hardware-in-a-loop CPS testbed. A demonstration is provided to show how the proposed defense systems can be deployed to protect a power grid against cyber intruders.

- Previous article in issue
- Next article in issue

Keywords

Cyber-physical system

Cyber security

Intrusion detection

CPS testbed

Smart grid

Abbreviations

ADS

Anomaly detection system

ADA

Advanced distribution automation

AMI

Advanced metering infrastructure

AMR

Automatic meter reading

ANSI

America National Standards Institute

CC

Control center

CCADS

Coordinated cyber attack detection system

CIP

Critical infrastructure protection

CPS

Cyber-physical system

CT

Current transformer

DA

Distribution automation

DER

Distributed energy resources

DMS

Distribution management system

DNP3

Distributed network protocol 3.0

DOE

Department of Energy

DoS

Denial of service

EMS

Energy management system

E-ISAC

Electricity Information Sharing and Analysis Center

ESCSWG

Energy Sector Control Systems Working Group

FCN

Field communication network

FDIR

Fault detection, isolation and recovery

FRTU

Feeder remote terminal unit

GOOSE

Generic object-oriented substation event

GPS

Global positioning system

HAN

Home area network

HMI

Human machine interface

HIDS

Host-based IDS

LAN

Local area network

MDMS

Meter data management system

MMS

Manufacturing message specification

MTTC

Mean-time-to-compromise

MU

Merging unit

NAN

Neighborhood area network

NERC

North American Electric Reliability Corporation

NIDS

Network-based IDS

NIST

National Institute for Standards and Technology

IADS

Integrated ADS

ICT

Information and communications technology

ICCP

Inter-control center communications protocol

IDPS

Intrusion detection and prevention system

IDS

Intrusion detection system

IEC

International Electrotechnical Commission

IED

Intelligent electronic device

IP

Internet Protocol

ISA

International Society for Automation

ISEAGE

Internet-scale event and attack generation environment

ISM

Industrial, scientific, and medical (radio bandwidth)

IT

Information technology

OMS

Outage management system

OPC

Object linking and embedding for process control

PDC

Phasor data concentrator

PLC

Programmable logic controller

PMU

Phasor measurement unit

RTDS

Real-time digital simulator

RTU

Remote terminal unit

SAS

Substation automation system

SAIFI

System average interruption frequency index

SAIDI

System average interruption duration index

SCADA

Supervisory control and data acquisition

SCL

Substation configuration language

SCT

Smart City Testbed

SDO

Standard Development Organization

SMV

Sample measured value

TO

Transmission operator

VT

Voltage transformer

WAMS

Wide area monitoring system

WAN

Wide area network

WSU

Washington State University

Recommended articles

Cited by (0)

View Abstract

Recommended articles

No articles found.