"Cyber-Physical Security : Protecting Critical Infrastructure at the State and Local Level", par Robert M. Clark & Simon Hakim

"Cyber-Physical Security : Protecting Critical Infrastructure at the State and Local Level", par Robert M. Clark & Simon Hakim

Anass Rabii
Siweb Research team, Ecole Mohammadia d'Ingénieurs, Univ. Mohammed V-Rabat – Maroc
anassrabiianass@gmail.com

Résumé

Le troisième volume de la série "Cyber-Physical Security" décrit les risques et vulnérabilités que courent les infrastructures gouvernementales critiques au niveau local en plus des mesures préventives. Ce livre s'adresse aussi bien aux responsables locaux qu'aux personnes intéressées par les politiques locales. Il synthétise les contributions de plusieurs experts du domaine.

Abstract

The third volume of the series "Cyber-Physical Security" describes cyber-security risks and vulnerabilities in the context of critical government infrastructure as well as preventive measures. This book is for both government officials and third parties interested in local policies. This books contains the culmination of contributions from many experts in the field.

Mots-clés

Cyber-Sécurité, Infrastructure critique, Gouvernement.

Keywords

Cyber-Sécurity, Critical Infrastructure, Gouvernment.

"Cyber-Physical Security" est un ouvrage publié en 2017 qui s'ajoute à la série de publications des chercheurs Robert M. Clark et Simon Hakim, pour fournir un guide complet des risques que courent les Infrastructures à Importance Vitale (IIV) ainsi que des techniques et contrôles pour y faire face.
Bien que l'ouvrage prenne le cas des États-Unis comme cadre de référence pour les infrastructures et le cadre judiciaire, les auteurs proposent un cadre général destiné à tous les gouvernements. Des études de cas mettent en valeur des approches nationales (Australie, Singapour, USA). L'ouvrage semble être destiné en premier lieu aux responsables gouvernementaux.
Le livre s'ouvre par la terminologie de la cyber sécurité et de la gestion des risques. Ensuite, deux standards majeurs à savoir ISO/IEC 27001 et NIST Special publication 800-82 sont présentés et comparés. La suite est structurée sous forme de contributions de plusieurs experts du domaine.
J'ai apprécié la structure des chapitres similaire à une succession d'articles qui les rend indépendants, plus faciles à lire et à accéder. L'ouvrage manque cependant de graphiques et d'illustrations, notamment pour une suite de processus ou pour une vue synthétique. Grâce aux nombreuses définitions, exemples illustratifs et au langage compréhensible, je recommanderais cet ouvrage à toute personne intéressée par la cyber sécurité, quelque soit son niveau d'expertise.