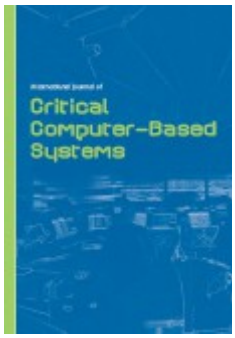

International Journal of Critical Computer-Based Systems

Special Issue on: "Resilience of Cyber-Physical Systems in Industry: Applications and Challenges"

Guest Editors:
Dr. Danilo Pelusi, University of Teramo, Italy
Dr. Janmenjoy Nayak, Aditya Institute of Technology and Management, India
Dr. Asit Kumar Das, Indian Institute of Engineering Science and Technology, Shibpu, India

Last two decade is witnessing an exceptional growth of cyber-physical systems (CPS), which are foreseen to modernize our world through the creation of new services and applications in a variety of sectors such as cloud computing, environmental monitoring, Big data, Cybercrime, E-health systems and intelligent transportation systems. Cyber-Physical Systems (CPSs) interrelate various physical world with digital computers and networks to facilitate automatic production and distribution processes. For remote monitoring and control, most of the CPS is not working in seclusion, but their digital part is connected with the Internet. Always there is a huge chance of getting unacceptably high residual risk in critical network infrastructures, though the impediment and monitoring measures may condense the cyber attacks risk. In such scenarios, Resilience helps to make able to the system to endure adverse events with the maintenance of an acceptable functionality. Also, the integration of CPS and Big data has emerged many new solutions for cyber attacks. The interconnection with the real-world, in industrial and critical environments, requires reaction in real-time. This Special Issue will focus on the latest approaches to novel Cyber-Physical System (CPS) resilience in real-world industrial applications. Moreover, it will fulfil the requirements of the resilience of CPSs in cross-discipline analysis along with real life applications, challenges and open issues involved with cyber-security threats. The SI will offer a clearly structured, highly accessible resource for a diverse application, including researchers and industry practitioners who are interested in evaluating and ensuring the resilience of CPSs in both the development and assessment stages.

Subject Coverage
Suitable topics include, but are not limited, to the following:

- CPS in fraud-detection systems
- CPS for smart phone security and privacy
- CPS in adversarial environments
- CPS in crime analysis
- CPS for attack detection in the smart grid
- CPS for smart health care system
- Risk Assessment of Cyber-Physical Systems
- Data analytics and processing platforms in CPS
- CPS in Blockchain systems
- Compliance Assessment of Industrial Automation and Control System
- Network security in IoT Platform
- CPS in Smart Industry
- Security and Secured systems in Smart city
- CPS in Bigdata platform
- AI based sensor Applications for IoT environment
- Development of Advance Intrusion detection system using CPS
- Machine learning in network intrusion systems

Notes for Prospective Authors
Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. (N.B. Conference papers may only be submitted if the paper has been completely re-written and if appropriate written permissions have been obtained from any copyright holders of the original paper).

All papers are refereed through a peer review process.

All papers *must* be submitted online. To submit a paper, please read our Submitting articles page.

If you have any queries concerning this special issue, please email the Guest Editors:
Dr. Danilo Pelusi: dpelusi@unite.it
Dr. Janmenjoy Nayak: mailforjnayak@gmail.com
Dr. Asit Kumar Das: akdas@cs.iiests.ac.in

Important Dates

Manuscripts due by: *31 January, 2021*

Notification to authors: *30 April, 2021*

Final versions due by: *30 June, 2021*