Nasser Abouzakhar, Ind Eng Manage 2014, 3:5
http://dx.doi.org/10.4172/2169-0316.S1.003

OMICS Group Conferences
Accelerating Scientific Discovery

International Summit on
Industrial Engineering
December 08-10, 2014 DoubleTree by Hilton Hotel San Francisco Airport, USA

Nasser S Abouzakhar
University of Hertfordshire, UK

Cyber security for industrial control and automation systems

Most of current industries and their critical infrastructure rely heavily on control systems and data networks for everything. The increase in the electronic services and operations for various industries has led to an increase in different threats and malicious activities. Recently, the security community have witnessed a significant increase in security threats on various critical industrial infrastructure and systems such as nuclear power utilities, oil and gas industry, nuclear power generation systems and petrochemical plants etc. During the last couple of years, emerging security risks and violations have been identified and have had a negative impact on critical industrial systems and services. Cyber security threats include such issues as energy and power generation failures, control systems malfunction, and hazardous material accidents. According to the BBC online news in December 2011, the FBI's cyber division released the news that the infrastructure systems of three US cities have been attacked. FBI reported that hackers managed to make their way into SCADA systems within one major city and had control of that city's system. Critical industrial systems must keep the operational environment safe, secure and resilient against constantly evolving cyber threats. This is to maintain the safety of workers, industrial assets as well as the communities they serve. Therefore, managing cyber security risks is a challenging task shared by all entities involved in developing, designing, operating and maintaining critical industrial infrastructure and systems. The purpose of this workshop is to bring together researchers, practitioners and industrials interested on security aspects related to industrial automation and control systems. Recent advances in the fields of industrial systems security such as control systems security and embedded systems security, software security and intrusion detection and prevention are a key factor in the growth of critical industrial operations and services. This workshop is expected to attract academics and professionals and to stimulate interesting discussions about the latest development of solution models and techniques for Industrial Automation Cyber Security.

Biography

Nasser S. Abouzakhar is a senior lecturer at the University of Hertfordshire, UK. Currently, his research area is mainly focused on critical infrastructure security, industrial control systems security and applying machine learning solutions to various Internet and Cyber security related problems. He received MSc (Eng) in Data Communications in 2000 followed by PhD in Computer Sci Engg in 2004 from the University of Sheffield, UK. Nasser worked as a lecturer at the University of Hull, UK in 2004-06 and a research associate at the University of Sheffield in 2006-08. He is a technical studio guest to various BBC World Service Programmes such as Arabic 4Tech show, News hour programme and Breakfast radio programme. Nasser is a BCS assessor for the accreditation of Higher Education Institutions (HEIs) in the UK, BCS chartered IT professional (CITP), CEng and CSci. His research papers were published in various international journals and conferences.

n.abouzakhar@herts.ac.uk