IEEE

IEEE Sensors Council
ITALY CHAPTER

2021 IEEE INTERNATIONAL WORKSHOP ON
METROLOGY FOR INDUSTRY 4.0 & IoT

ROME, ITALY / JUNE 7 - 9, 2021

METROIND4.0&IoT

CALL FOR PAPERS for the Special Session on

CYBERSECURITY STANDARDS AND TECHNOLOGIES FOR IOT AND INDUSTRY 4.0 (SECURITYSTANDARDS)

ABSTRACT

CyberSecurity is a critical issue for the viability of the Internet of Things and Industry 4.0. Security breaches lead to serious impacts on the well-being of the citizen, on the operation of industries, and on the stability of nations. The impact of security breaches in all dimensions of the Society has led more and more countries to understand CyberSecurity as a State issue - and therefore to investigate strategies to address CyberSecurity in a systematic and effective manner.

SecurityStandards Special Session at the IEEE International Workshop on Metrology for Industry 4.0 and IoT aims at discussing how to address CyberSecurity via the use of international standards. SecurityStandards seeks advances in two dimensions, as we discuss next.

Security Requirements. How to establish standards and requirements for equipment, systems and professionals in the area of security. How to assess the risks associated with each field of application. How to define the sectors in which the State must intervene by establishing mandatory safety requirements.

Security Assessment. How to verify compliance with safety requirements by equipment, systems and professionals. Which tests are most effective to characterize the fulfillment of such requirements. Which conformity assessment schemes are best suited to each scenario. How to attest the competence of professionals and laboratories to carry out security assessment activities.

ORGANIZERS

Alan **Oliveira de Sá**

*Admiral Wandenkolk
Instruction Center
Brazilian Navy, Brazil*

Lucila Maria **de Souza Bento**

*Inmetro - National Institute
of Metrology, Quality and
Technology, Brazil*

CONTACTS

www.**metroind40iot**.org

info@**metroind40iot.org**

facebook.com/**MetroInd40IoT**

TOPICS

In this sense, SecurityStandards seeks original contributions on the following themes:

Standards and Conformity Assessment
- Security standards for software and smart devices
- Conformity assessment methods for cybersecurity
- Information security management systems standards
- Risk assessment standards
- Accreditation of security assessment laboratories

Security Requirements
- Cryptography Standards
- Software Applications
- Smart Devices
- Management Systems
- Professional Competence
- Security in new paradigms: Cloud, IoT, Cyber-Physical
- Privacy and Confidentiality Requirements

Hardware Security
- Side-channel attacks and countermeasures
- Fault attacks and countermeasures
- Hardware tampering and tamper-resistance
- Hardware and software reverse engineering
- Trusted computing platforms
- Secure storage devices
- Cryptographic processors and co-processors
- True and pseudorandom number generators
- Physical unclonable functions

Risk Management and Critical Infrastructure Applications
- Energy
- Water and Sewage
- Transportation
- Communication
- Financial System
- Public Security and Civil Defense

Software Security
- Static code analysis
- Dynamic software analysis
- Software Testing
- Code obfuscation
- Software incorruptibility
- Software watermarks
- Software validation
- Reference datasets

Visit the conference website as well as Facebook page for each specific call and additional news.

www.metroind40iot.org/special-session-2
info@metroind40iot.org