Announcement

Industry 4.0 SCIENCE

IoT Security

The growing connectivity of machines, systems, and products is creating new opportunities for data-driven production, but it is also expanding the attack surface of industrial environments. As the Industrial Internet of Things (IIoT) becomes increasingly integrated into manufacturing and logistics, protecting connected devices, communication networks, and industrial data is pivotal for the successful transition to Industry 4.0. How do we combine connectivity, interoperability, and operational efficiency with robust cybersecurity?

Industrial IoT security requires a holistic approach that extends beyond individual devices and technical safeguards. Network architectures, access control, data integrity, software updates, and the management of vulnerabilities throughout the life cycle all play an important role. At the same time, the convergence of information technology (IT) and operational technology (OT) creates new dependencies and security risks. Companies must address these challenges without compromising the availability, reliability, and real-time capabilities essential to industrial processes.

This issue of Industry 4.0 Science (www.industry-science.com) highlights current approaches, technologies, and strategies for connected and secure industrial environments. By bringing together technical solutions and organizational perspectives, the issue explores how cybersecurity can become an integral part of resilient, trustworthy, and sustainable Industry 4.0.

Industry 4.0 Science, Issue 3/2027
Publication **June 10, 2027**

Editor of the Issue

Prof. Norbert Gronau
Chairman of the I4S Editorial Board
University of Potsdam

GITO

Want to help us drive Industry 4.0 forward and publish your own issue?
Applications for guest editorship can be submitted to editorial-office@industry-science.com