

CALL FOR PAPERS



IEEE Transactions on Industrial Informatics



Special Section on:

“Security in Industrial Networks”

Special Section Guest Editors

Luca Durante
IEIIT-CNR
Italian National Research Council
C.so Duca degli Abruzzi, 24
10129 Torino, Italy
phone: +39 011 564 5425
fax: +39 011 564 5429
luca.durante@polito.it

Adriano Valenzano
IEIIT-CNR
Italian National Research Council
C.so Duca degli Abruzzi, 24
10129 Torino, Italy
phone: +39 011 564 5410
fax: +39 011 564 5429
adriano.valenzano@polito.it

Background: For a very long time industrial networked systems, such as for instance process control systems (PCSs), supervision, control and data acquisition (SCADA) systems and factory communication systems have been considered “secure”, or, at least, security was not perceived as a primary issue in those scenarios, especially when compared to reliability, performance and fault-tolerance. In the last years, however, things have been changing rapidly and dramatically, mainly because of two kinds of reasons. On the one hand, the need for accessing more and more information in real-time directly from plants, controlled processes or manufacturing systems, just to mention some significant examples, has pushed companies and organizations to interconnect their industrial and corporate networks through public communication systems and the Internet, in particular. While this has enabled very attractive opportunities for remote monitoring, control, maintenance and assistance offering functionalities that are no longer limited by any “on-site” presence, it also exposes the industrial systems to the same security threats and attacks that are typical of general-purpose computer networks.

On the other hand, industrial devices, that in the past were mainly based on proprietary and *ad-hoc* solutions for both their h/w and s/w components (i.e. PLCs and NCs), now tend to include more and more elements borrowed from the traditional ICT domains such as (open-source) operating systems, communication protocols, network interface cards and so on. Besides obvious advantages, however, this also introduces vulnerabilities in those devices that can be exploited by malicious agents, hackers and cyber-criminals.

This situation is made even more critical by the adoption of wireless communication technologies in an increasing number of industrial distributed applications that could represent new appealing opportunities for attackers to access their target systems.

This Special Section on “Security in Industrial Networks” aims at presenting some of the most significant research works focusing on security issues in industrial networks (including all kinds of automation networks, PCSs, SCADAs, factory communication systems, critical infrastructure control and management networks and so on) and representing the current state-of-the-art. Topics include, but are not limited to, the following:

- *Techniques and tools for the specification, modeling and analysis of network security, including techniques based on formal methods, approaches relying on simulation and/or emulation, modeling and analysis of attacks and countermeasures.*
- *Security of networks and protocols for industrial applications, including distributed control systems, industrial and building automation, plant and large infrastructure management.*
- *Security requirements including availability and tolerance to attacks.*
- *Security in wireless networks, wireless sensor networks, wireless (sub)networks for management, monitoring and diagnostics and wireless networks for automation.*
- *Performance evaluation and measurement of security-oriented networking solutions, performance-security tradeoffs.*
- *Risk assessment and management in industrial networks, testing, audits and metrics for industrial networks security.*
- *Case studies and applications of innovative solutions to enhance the security of industrial networks. Case studies of actual attacks.*

Submissions to this Special Section must represent original material that have been neither submitted to, nor published in, any other journal. Extended versions of papers previously published in conference proceedings, digests or preprints may be eligible for consideration, provided that the authors inform the Special Section Guest Editors at the time of submission.

Manuscript preparation and submission: Follow the guidelines in “Information for Authors” in <http://iee-ies.org/tii/>
Submit using Manuscript Central only
<http://mc.manuscriptcentral.com/tii>

Paper submission deadline: September 30, 2009

Expected publication date: August 2010 (tentative)

Note: The recommended papers for the section are subject to final approval by the Editor in Chief. Some papers may be published outside the special section, at his discretion.