ISTITUTO
DI TECNOLOGIE DELLA
COMUNICAZIONE,
DELL'INFORMAZIONE
E DELLA
PERCEZIONE

Sant'Anna
Scuola Universitaria Superiore Pisa

ESTEP

SAVE THE DATE

# 7 - 8 October 2019
# Pisa, Italy

The Focus Group Smart Factory of the European Steel Technology Platform is proud to present the workshop:

# Cybersecurity in the steel industry
# Threats, risks and impact on the steel companies

The workshop is dedicated to key players such as steel manufacturers, systems integrators, solution providers, academic and R&D experts focusing management of threats, risk evaluation, defense policy and mitigation strategies evidencing the impact on business in general and the operational environment for humans and systems.

**Participation fee**

Participation fee is 200 €. It will include workshop proceedings, common dinner / lunch and coffee breaks.
Payment instructions will follow with the detailed Program of the two days, the location address and the list of suggested accommodations

**Sponsorship opportunities**

Companies interested in exhibiting and/or sponsoring the event may contact the ESTEP Organising Secretariat : D.Snaet@estep.eu

# 7 - 8 October 2019
# Pisa, Italy

## Background

The increasing interconnection of equipment, systems and humans is exposing the steel industry to new threats and risks even in the manufacturing operational technology (OT). While the IT community is already aware and alerted about the importance of cybersecurity, corresponding concepts and the need to fortify against intentional sabotage slowly transfers to operational technology.

Moreover, the evolution of digitalization is increasing the probability of production failures and loss of sensitive data due to cyber-attacks and data hacking. Human errors in production operation also have to be considered regarding data integrity and protection. This leads to consider cybersecurity at the same level of importance as production efficiency, quality and continuity of production processes. In the past, directed attacks have damaged equipment. Modern threats involve latent attacks resulting in continuously process quality reduction while remaining hidden and undetected.

## Topics

Experts, ICT engineers and managers, solution providers and system integrators, suppliers, universities and research institutes, consulting companies, national and international organisations operating in steel and other industrial sectors are invited to submit abstracts on cybersecurity-related topics relevant to the steel context such as the ones reported in the following not exhaustive list:

- Industrial needs for the Cyber-threats and R&D directions in Cybersecurity
- Continuous Monitoring of networks and systems
- Cyber menaces, threats and risks; Risk Analysis examples in the Process Industry and other industrial sectors
- Cybersecurity and legacy systems
- Organisation and technological policy for increasing Cybersecurity in the Supply Chain and Operations
- Standards and Cybersecurity Capability Management Models in Process Industry
- Impact of Cybersecurity: workforce, operations, systems and organization
- Examples and Experiences.

## Deadlines

Submission of abstracts July 15, 2019 - To be sent to D.Snaet@estep.eu

Information on acceptance August 15, 2019

Opening of the online registration September 1, 2019