



ICAM26

International Conference on Advanced Manufacturing

Research to Application through Standardization

ORLANDO, FL
SEPTEMBER 28 - OCTOBER 2, 2026

Industry 4.0 : Security, Trust, and Cyber Resilience

As use of AM equipment continues to grow and be more interconnected with Industry 4.0, the risks of cyber and cyber-physical attacks is increasing, including threats such as intellectual property theft, counterfeit products and the illicit production of 3D-printed weapons. These threats pose significant challenges to safety, economic stability, and supply chain security. Traditional security measures might not always be adequate, requiring a comprehensive approach that addresses digital rights management, design protection, and the potential misuse of AM technology. Strengthening AM security will enhance trust in AM-produced parts and support wider adoption. This symposium examines these security concerns within the evolving Industry 4.0 landscape.

Topics of interest include but are not limited to:

- Connectivity and security of AM networks
- Mitigation methods and solutions to enhance security for AM
- The extent to which general Operational Technology cyber-security guidance applies to AM
- Security across the AM supply chain from design to manufacturing
- AM and threats to Intellectual Property
- Standards and needs for AM security
- The legality of 3D Printed weapon components and fully printed devices
- Security of AM supply chain, design IP and 3rd party risk protection
- New and novel risks and abuses of counterfeiting products



amcoe.org/icam2026

SYMPORIUM CO-ORGANIZERS

Chris Adkins
Materialise, USA

Narasimha Annapareddy
Texas A&M University, USA

Thomas Chittum
Chittum Law, USA

Paul Foley
StockX, USA

Mark Yampolskiy
Auburn University, USA

ASTM STAFF CONTACT

Paul Bates
ASTM International