ICAM25

International Conference on Advanced Manufacturing

Research to Application through Standardization

October 6-10 | Las Vegas, NV

Industry 4.0: Security Aspects

As AM equipment becomes more interconnected with Industry 4.0, the risks of cyber and cyber-physical attacks grow, including threats such as intellectual property theft and the illicit production of 3D-printed weapons. These threats pose significant challenges to safety, economic stability, and supply chain security. Traditional cybersecurity 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
– Cyber Security of AM equipment
– Security across the AM supply chain from design to manufacturing
– Novel attacks
– 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
– Insider threats to AM security

Symposium Organizers

– **Chris Adkins**, Materialise, USA
– **Narasimha Reddy**, Texas A&M University, USA
– **Thomas Chittum**, SoundThinking, USA
– **Darrick Kristich**, Sedara, USA
– **William Ryan**, ATF, USA
– **Mark Yampolskiy**, Auburn University, USA

Submit an abstract

amcoe.org/icam2025