# SaTC-EDU: Collaborative: Cybersecurity Education for Additive Manufacturing

NYU Center for Cybersecurity

## Challenge:

- Develop resources on the topic of manufacturing cybersecurity for students and professionals
- Provide hands on experience with hackathon challenges

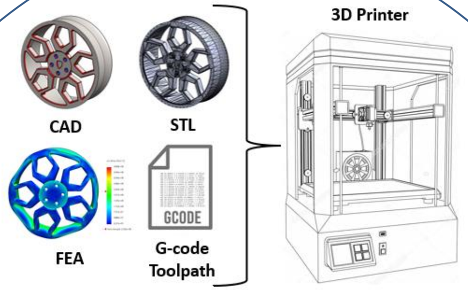
## Solution:

- Hack3D – student competition on manufacturing security
- Webinars – gathering of manufacturing cybersecurity community

DGE-1931724

New York University – Nikhil Gupta and Ramesh Karri

NY City College of Technology – Xiangdong Li and Gaffar Gailani



Additive Manufacturing process involves digital design files to create printed part

| Attack Goals | Attack Methods | Attack Targets |
|---|---|---|
| • Piracy<br>• Sabotage<br>• Counterfeiting<br>• Reverse engineering | • Denial of Service<br>• Tamper Data<br>• IP Theft<br>• Side Channel | • CAD designs<br>• AM Machine<br>• Sensors<br>• Controllers<br>• Data stream |

Hidden threats in the AM digital process chain

**Goal**: Train engineers to confront cybersecurity challenges during product design, development, and manufacturing

## Scientific Impact:

- Educate a new group of workforce with multidisciplinary knowledge
- Build a library of educational resources for both students and professionals

## Broader Impact and Broader Participation:

- Bridge gap in engineering and cybersecurity disciplines by developing a comprehensive education and training initiative
- Worked with over 1000 people in multiple events