Cyber-Physical System Security for Advanced Manufacturing

VANDERBILT

Virginia Tech

Acknowledgement
This work is sponsored by the NSF & DHS under the research award CNS1446303

Jaime Camelio, Jules White, Chris Williams, Lee Wells, Logan Sturm, Yao Pan, Dominic Ju

Towards a framework for comprehensive manufacturing cyber-attack risk assessment and detection

Problem

How vulnerable is our manufacturing infrastructure to undetected cyber-attacks that purposely change the design and manufacturing of parts so that the finished products deviate from their designed performance characteristics and fail in the field? Can attackers inject a design or manufacturing process change that goes undetected and causes a turbine blade for a jet engine to fail under a rare, but high load that should be within its designed tolerances? Is it possible that the phantom Toyota acceleration issue was actually the result of a purposefully injected manufacturing design change in a subset of their manufactured vehicles?

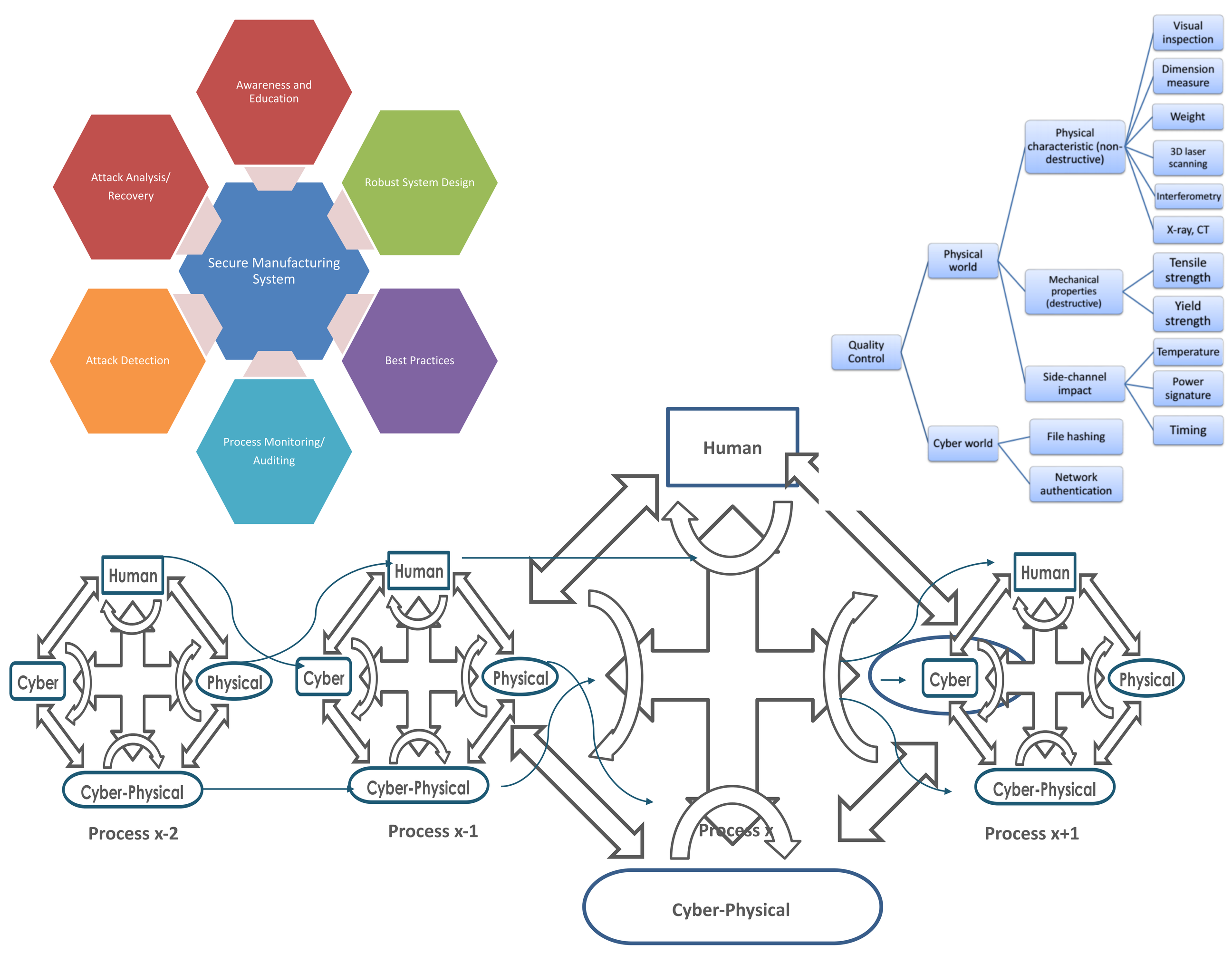
Solution Approach

Vulnerability – Any Potential Loss of Design Intent
- Intentional or Unintentional

Standard Framework to Discover Vulnerabilities
- Generic enough to encompass all manufacturing systems
- Should not require expert knowledge of individual processes/sub-systems

Considerations
- System complexity

Risk Assessment
- Constraint-based analysis of process, quality control, cyber-dimensions, and threat surfaces
- Design-space recommendations to improve process quality control to account for cyber-threats

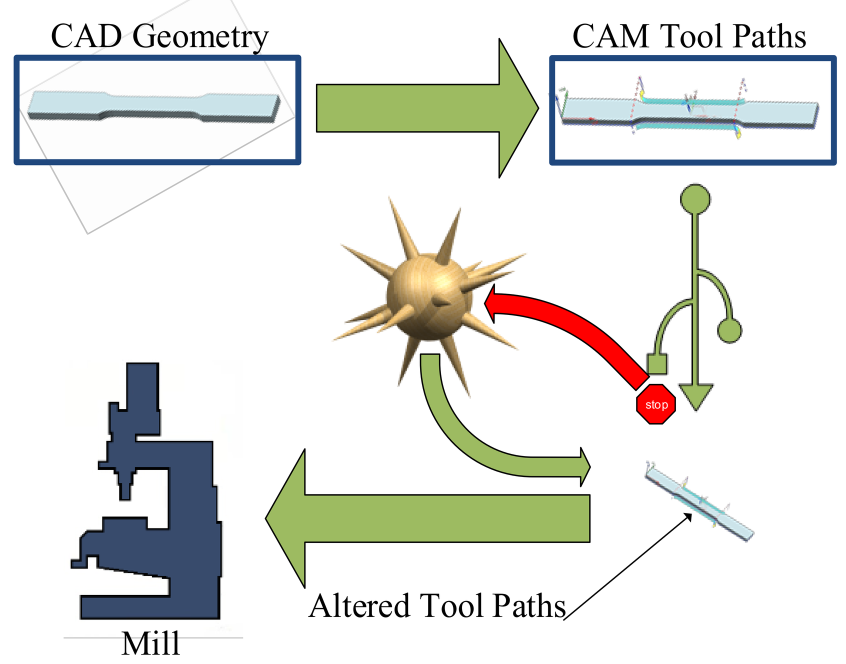


Subtractive Attack Feasibility

Goal: Exploit vulnerabilities in the Computer Aided Design and Manufacturing (CAD/CAM) process via malicious cyber-attacks to disrupt the design process or adversely affect a product's performance, quality, or end-user perceived quality

Demonstrate Attack Feasibility
- CAD/CAM
- Visual inspection
- Dimensional inspection
- Performance test

Understand Diagnostic Procedure of Unaware Engineers/Operators



Engineering Students Tasked to:
- Create an ASTM Compliant Tensile Test Specimen using CAD
- Generate Tool Paths to Machine the Specimen using CAM
- Transfer the Tool Paths to a PC Controlled Mill
- Machine the Specimen

Malicious Software
- Located on PC Controller
- Detects File Transfers
- Replaces Tool Paths Files

Outcome
- Incorrect Part Manufactured
- 19% Reduction in Performance

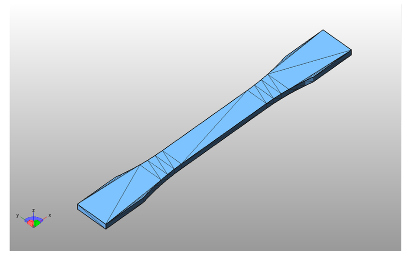
Additive Attack Feasibility

Determine where to place a void

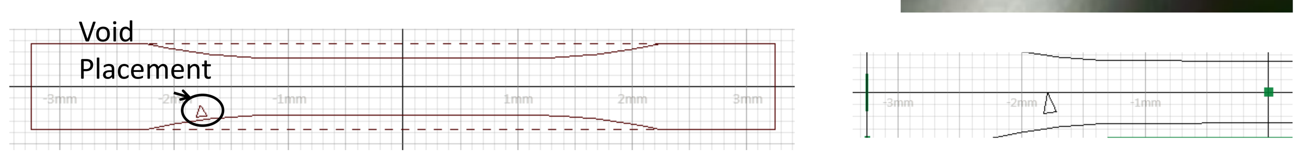
Stress concentration areas

Malware automatically searches for densest mesh areas (most likely to be stress concentration points)

Ray tracing used to determine if a point is within the mesh

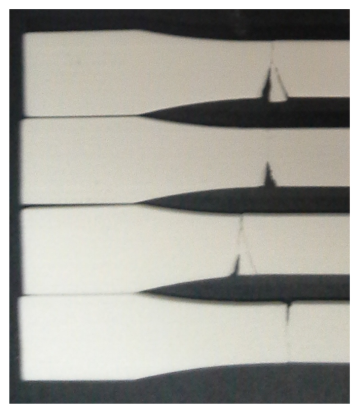


Dogbone parts

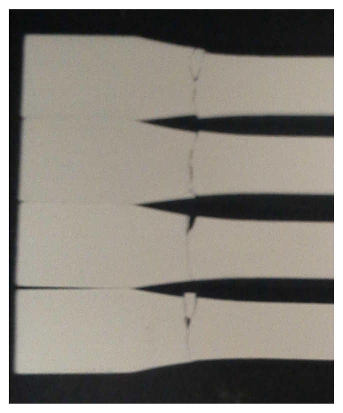


Fractures occur at the void locations

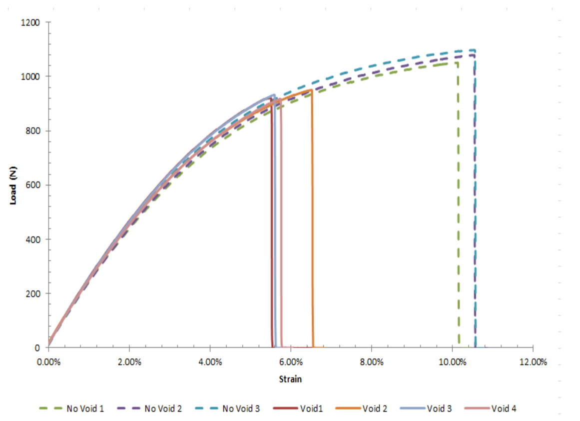
Without Void



With Void



Total load and strain decreased



Selected Publications

1. Hamilton Turner, Jules White, Brandon Amos, Jaime Camelio, Chris Williams, and Robert Parker. "Bad Parts- Are Our Manufacturing Systems At Risk of Silent Cyber-attacks?" IEEE Security & Privacy (to appear)
2. L. D. Sturm, C. B. Williams, J. Camelio, J. White, and R. Parker, 2014, "Cyberphysical Vulnerabilities in Additive Manufacturing Systems," International Solid Freeform Fabrication Symposium, Austin, TX., August 4-6
3. Jaime Camelio, Lee J Wells, Christopher B Williams, Jules White, Cyber-Physical Security Challenges in Manufacturing Systems, Manufacturing Letters, Volume 2, Number 2, pp. 74-77, 2014
4. Sam Hurd, Carmen Camp, Jules White, Quality Assurance in Additive Manufacturing Through Mobile Computing, The 7th EAI International Conference on Mobile Computing, Applications and Services, Nov 12-13, 2015, Berlin, Germany