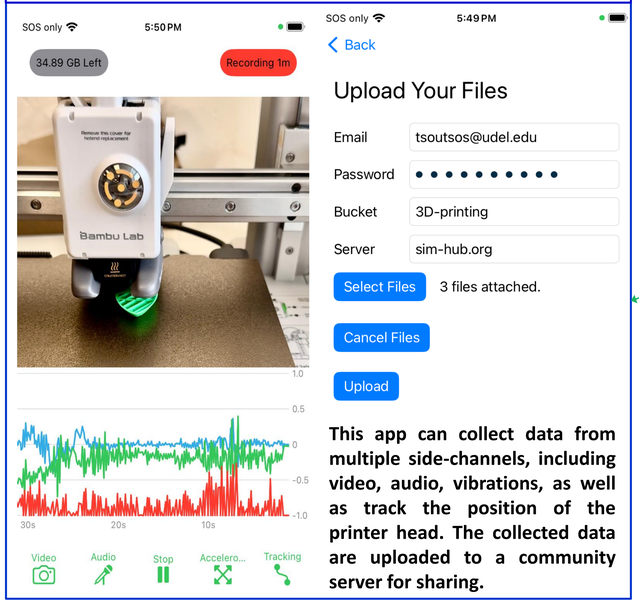
Data-Driven Cybersecurity Research Infrastructure for Smart Manufacturing

Smartphone App for Crowdsourced Data Collection



This app can collect data from multiple side-channels, including video, audio, vibrations, as well as track the position of the printer head. The collected data are uploaded to a community server for sharing.

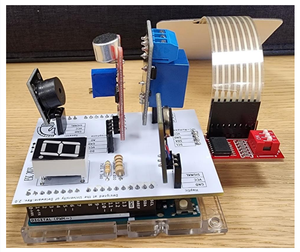
3D printers for data collection with anti-side channel features

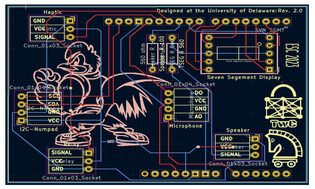
Vibration Compensation

Noise Cancellation

International competition on Cyber-Physical Systems

Embedded Security Challenge





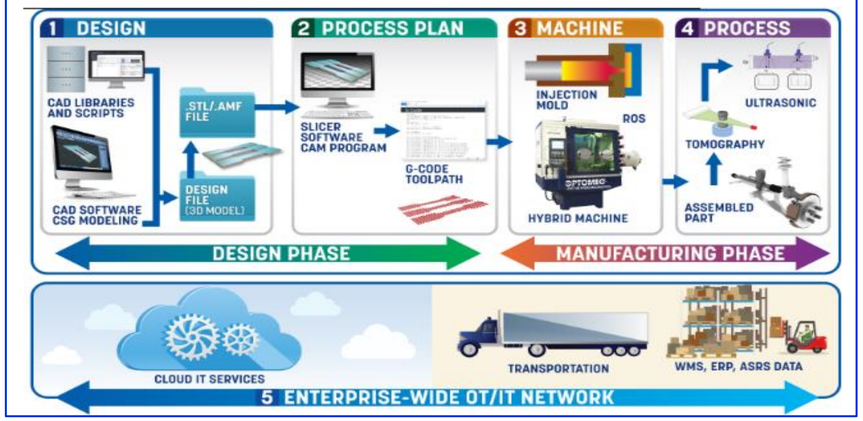
This year's ESC focuses on side channel attacks (SCA) on cyber-physical systems (CPS). The qualified teams are investigating a range of SCAs using a custom PCB and an Arduino Uno based CPS running several challenges that expose various side channels.

Research Vision and Mission

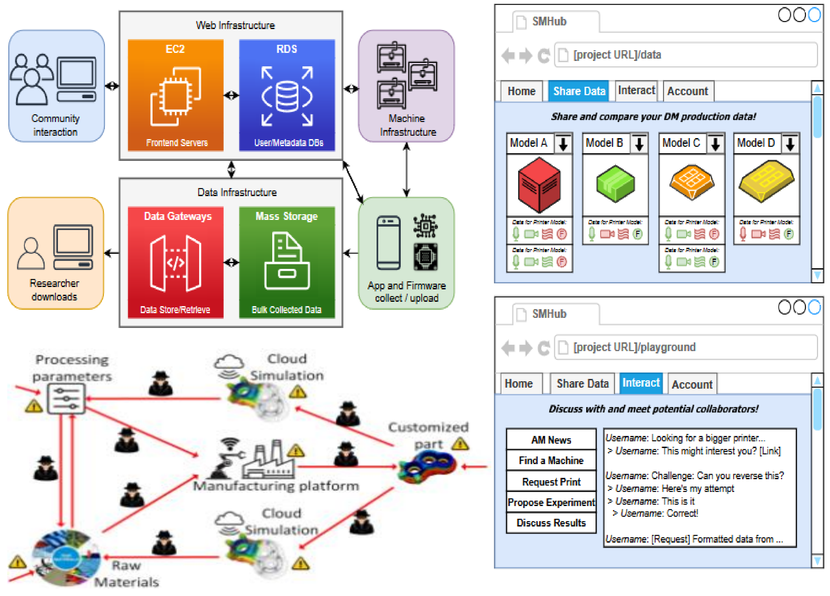
Creation of a Vibrant CISE Research Community for a Data-driven Cybersecurity for Smart Manufacturing (SM)

- Web Infrastructure
- Data Infrastructure
- SM Machine Infrastructure

SM Stages of Product Life Cycles and SM Hub



Community SM Infrastructure, SM Security Threats Risking Data Inputs and Communications with other entities, and SM Hub

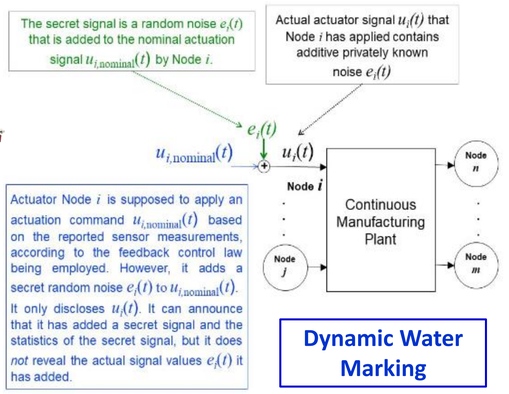


TAMU Smart Hybrid Machine (SHM) Platform

Siemens 828D Controller

Optomec MTS 500 Hybrid Machine

Digital Twin for Siemen's Sinumerik 828D Controller



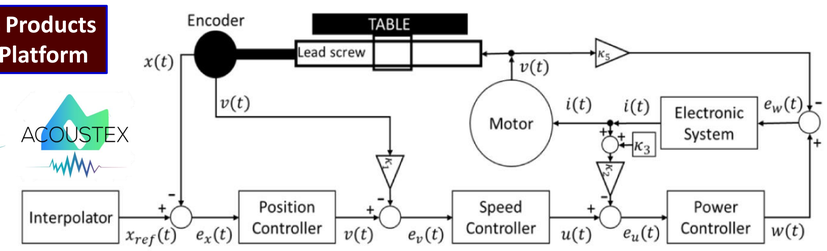
Dynamic Water Marking

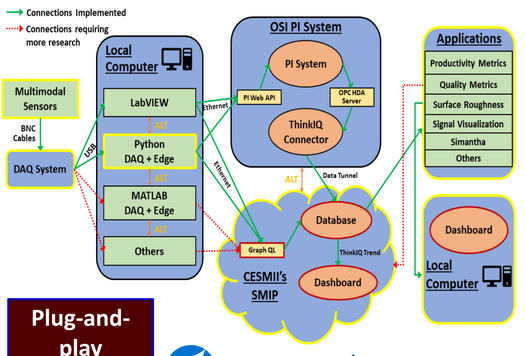
2 NSF i-Corps Products and 1 MaaS Platform

AlignAI FusionPro

ACOUSTEX

HiveAM designer





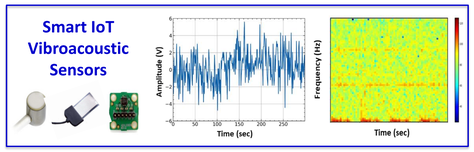
Plug-and-play Architecture with CESMII SMIP

OSIsoft. OPC UA

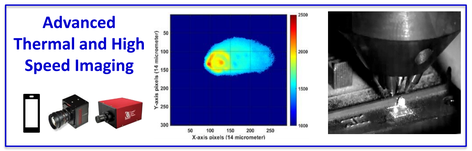
CESMII THE SMART MANUFACTURING INSTITUTE

Smart Sensor Wrapper (14+ channels)

Smart IoT Vibroacoustic Sensors



Advanced Thermal and High Speed Imaging

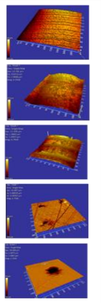
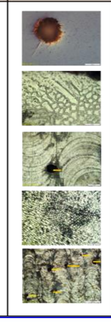
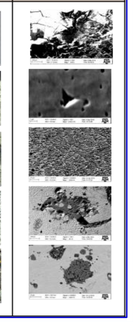


Machine Variable Logs via OPC UA Data Logger

Events

Event Log

Around 10 TB worth Multimodal Data from various printing materials and conditions

Data Source	Type of Data Collected	Data Rate (MB/min)	Data Volume (GB)	Characterization: 3D Optical Profilometer (800 KB per capture)	Characterization: Optical Microscope (10 MB per capture)	Characterization: SEM (1 MB per capture)
Accelerometer	Sensor time-series data via National Instrument's Data Acquisition System (NI-DAQ)	1.87	10			
Acoustic Emission		30	160			
Thin film		0.23	1.23			
Stratonics ThermaViz	In-situ melt pool history captured in form of raw frames and associated intensity-based data	1116	5972			
Photron High Speed Camera	High FPS (~6400) videos are recorded. Amount of time capture X FPS is always limited to < 174698 fames. For ex: At 5000 FPS, a 35 seconds of process will be captured.	1661	111			
Optical Camera	Process history captured via smartphone at 30/60/120 FPS	26.88	143			
Open Platform Communications (OPC)	Machine Log data keeping track of various machine variables such as XY coordinates of the table, status of the spindle, etc. in form of an Excel-based log	0.02	1			

References

- Wang *et al.*, "Implementing an open-source sensor data ingestion, fusion, and analysis capabilities for smart manufacturing.", *Manufacturing letters* (2022)
- Hanchate *et al.*, "HiRA-Pro: High resolution alignment of multimodal spatio-temporal data: a process physics driven approach.", *Journal of Computing and Information Science* (2023+), under review
- Karthikeyan *et al.*, "In-situ surface porosity prediction in hybrid-directed energy deposition process using explainable multimodal sensor fusion.", *Additive Manufacturing* (2023+), under review
- Tiwari *et al.*, "Protection against counterfeiting attacks in 3d printing by streaming signature-embedded manufacturing process instructions.", *In Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security* (2021)
- Tiwari *et al.*, "Cybersecurity assurance in the emerging manufacturing-as-a-service (MaaS) paradigm: A lesson from the video streaming industry.", *Smart and Sustainable Manufacturing Systems* (2020)
- Tiwari *et al.*, "A Survey of Cybersecurity of Digital Manufacturing.", *Proceedings of the IEEE* (2020)
- Hack3D | CSAW. https://www.csaw.io/hack3d (2020)
- Gouert *et al.*, "CSAW 2020 Embedded Security Challenge.", Available: https://github.com/TrustworthyComputing/csaw_esc_2020 (2020)
- Satchidanandan *et al.*, "Dynamic watermarking: Active defense of networked cyber–physical systems.", *Proceedings of the IEEE* (2016)
- Tsoutsos *et al.*, "Secure 3D printing: Reconstructing and validating solid geometries using toolpath reverse engineering.", *In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security* (2017)
- Tsoutsos *et al.*, "System and method for malware detection in additive manufactured parts.", *US Patent App.* (2019)
- Zheng *et al.*, "Towards improving data validity of cyber-physical systems through path redundancy.", *In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security* (2017)
- Zheng *et al.*, "IoTAegis: A scalable framework to secure the internet of things.", *In 2018 27th International Conference on Computer Communication and Networks (ICCCN)* (2018)