Secure Smart Manufacturing Testbed

using IIoT, Machine Learning, 5G and Zero Trust

Wesley Larrabee | Michael Laffin | Lee Kottke | Neil Borden | Scott Bresnahan

Advisors: Dr. Holly Yuan, Dr. Wei Shi, Brandon Cross, Aaron Bialzik, University of Wisconsin – Stout

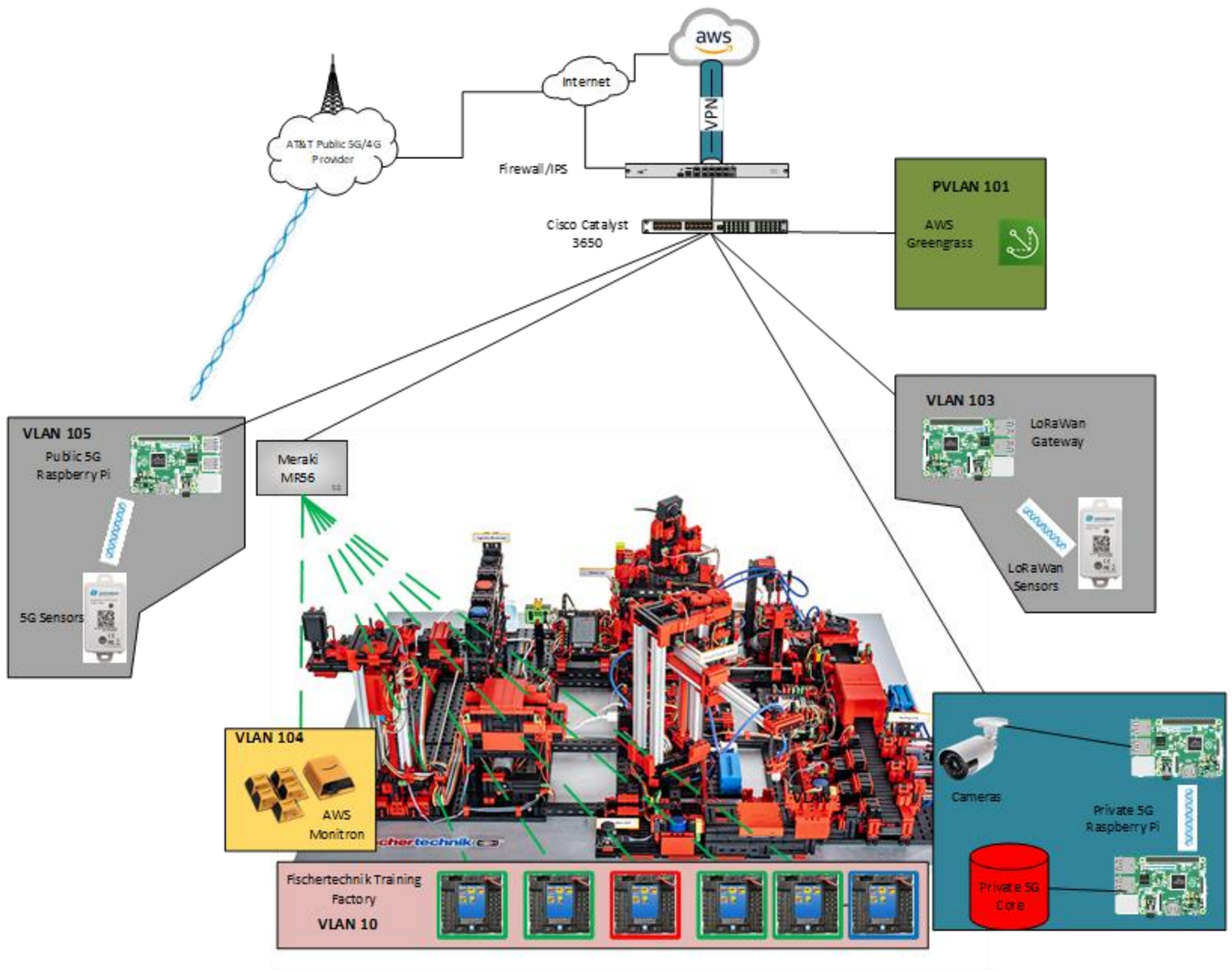
Sponsored by Department of Defense NCAE in Cybersecurity Curriculum and Research 2020 Program

Problem Statement

- Recent innovations in manufacturing have increased the interconnectivity of machines and physical equipment
- This enables greater throughput of manufacturing data which can be used to optimize production and reduce human intervention
- *Security vulnerabilities are commonly introduced during establishment of a Smart Factory*

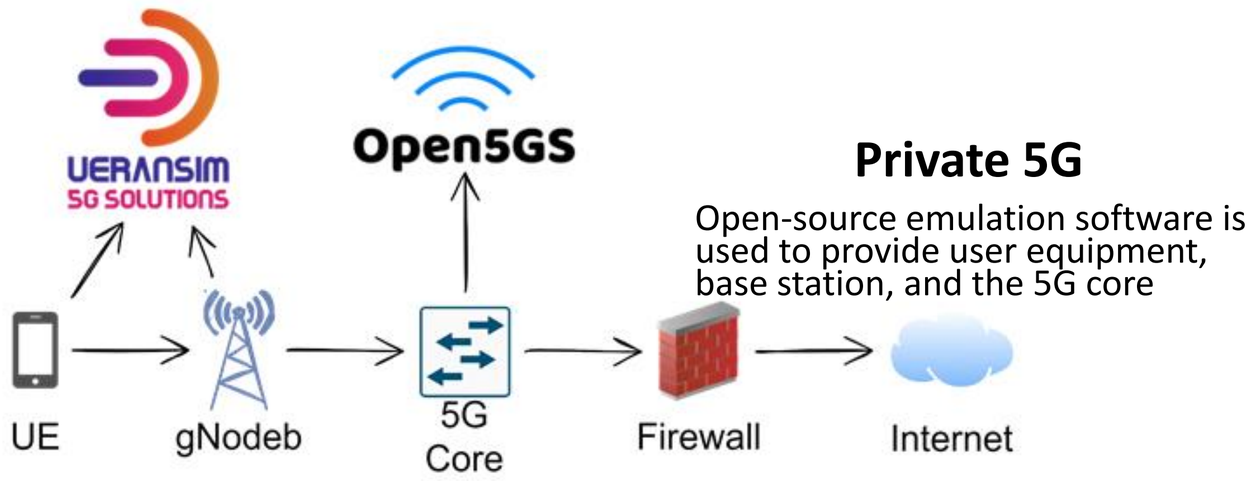
Objectives

- Emulate smart manufacturing technologies including Industrial Internet of Things (IIoT), 5G, Machine Learning and predictive maintenance
- Secure the smart factory with the zero-trust model



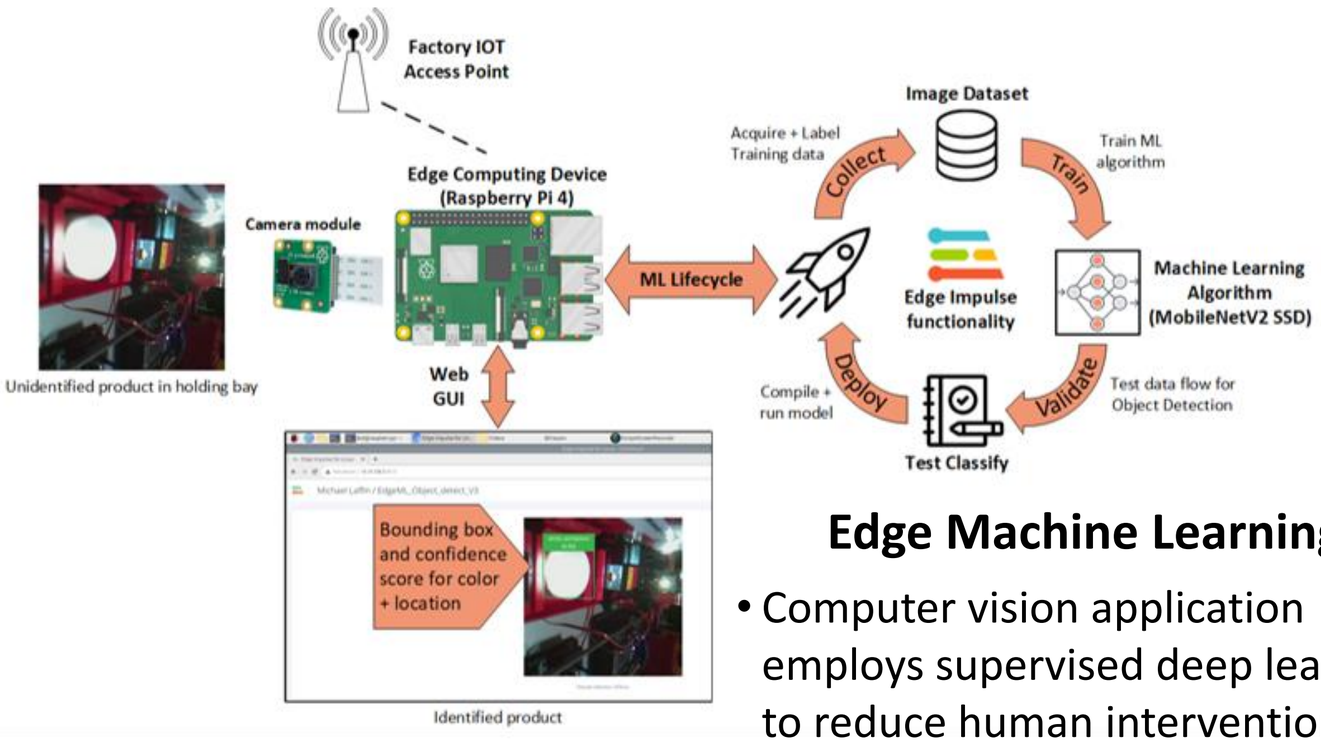
Implementation

A Fischertechnik Training Factory served as a physical testbed on which intelligent data processing capabilities and secure networking functionality were added.



Private 5G

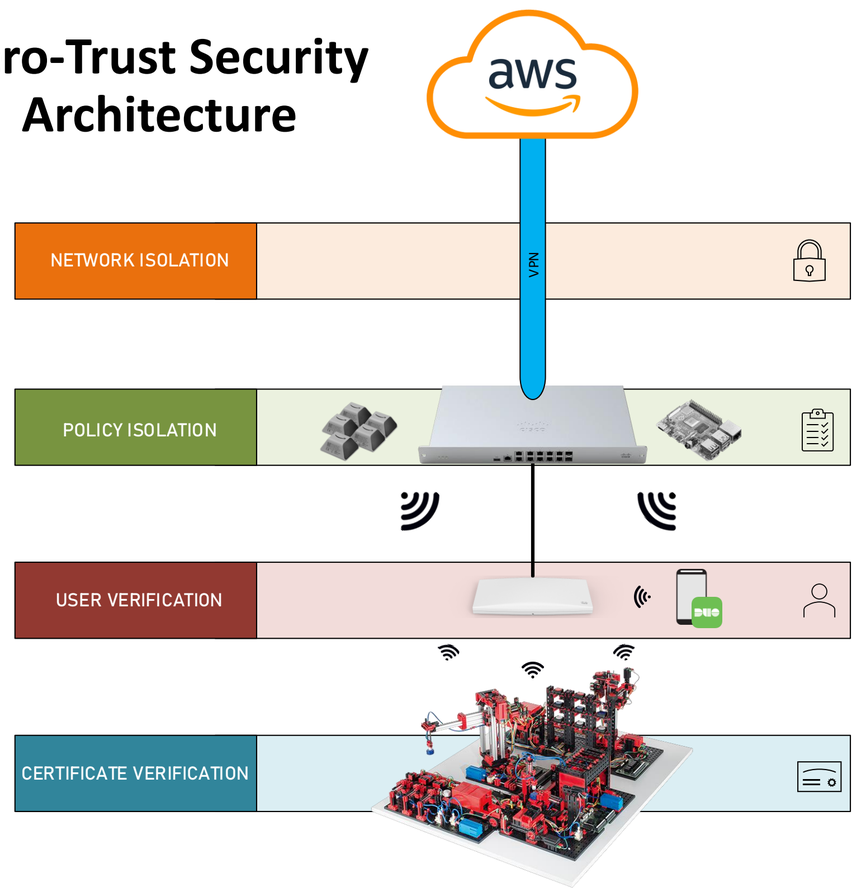
Open-source emulation software is used to provide user equipment, base station, and the 5G core



Edge Machine Learning

- Computer vision application employs supervised deep learning to reduce human intervention during quality-control
- Local processing reduces cloud network traffic

Zero-Trust Security Architecture



Future Work

- Organize and deliver seminars and hands-on workshops to local manufactures and show business use cases where a smart factory can drive value.
- Write and disseminate Industry 4.0 educational materials to the education community.