Multidisciplinary Engineering Capstone Project: Fall 2023 - Spring 2024

Small-Scale Factory Testbed for Cybersecurity Analysis

GOAL:

Enable the cybersecurity analysis and evaluation of factory systems with accurate virtual/real testbeds.

BACKGROUND:

Modern manufacturing systems and production lines are composed of many diverse devices, systems, networks, and software that may be vulnerable to cyber-attack. Securing these modern factory floors requires continuous detailed analysis and execution of what-if scenarios. Such detailed analysis and execution of what-if scenarios cannot be performed on actual production systems. Hence, adequate models, testbeds, and digital twins of factory floors and their respective supporting cyber-systems are needed.

OBJECTIVES:

This capstone team will analyze, design, and strive to implement a small-scale prototype factory cybersecurity lab consisting of a combination of hardware, networking, and software systems capable of emulating and replicating a small-scale factory process in a generic modern factory for evaluation purposes. An example, but not necessarily the final solution, would be a 3D virtual environment capable integrating a combination and virtualized and physical devices in a factory floor environment and their connectivity. This visualization could be enhanced with simulated data from the factory floor, for example, speed of production or other information helpful to the cybersecurity analysis of the status of the factory.

HARDWARE and SOFTWARE ENVIRONMENTS:

Simulation environments and libraries; Robot and factory simulation libraries; Graphics visualization engines; Powerful computer workstation. We plan on using GitHub and MS Teams for collaboration.

CUSTOMER:

Coordinator for UI: Daniel Conte de Leon, University of Idaho.

EXPECTED TEAM:

A team of dedicated Computer Science, Cybersecurity, and Mechanical Engineering students.

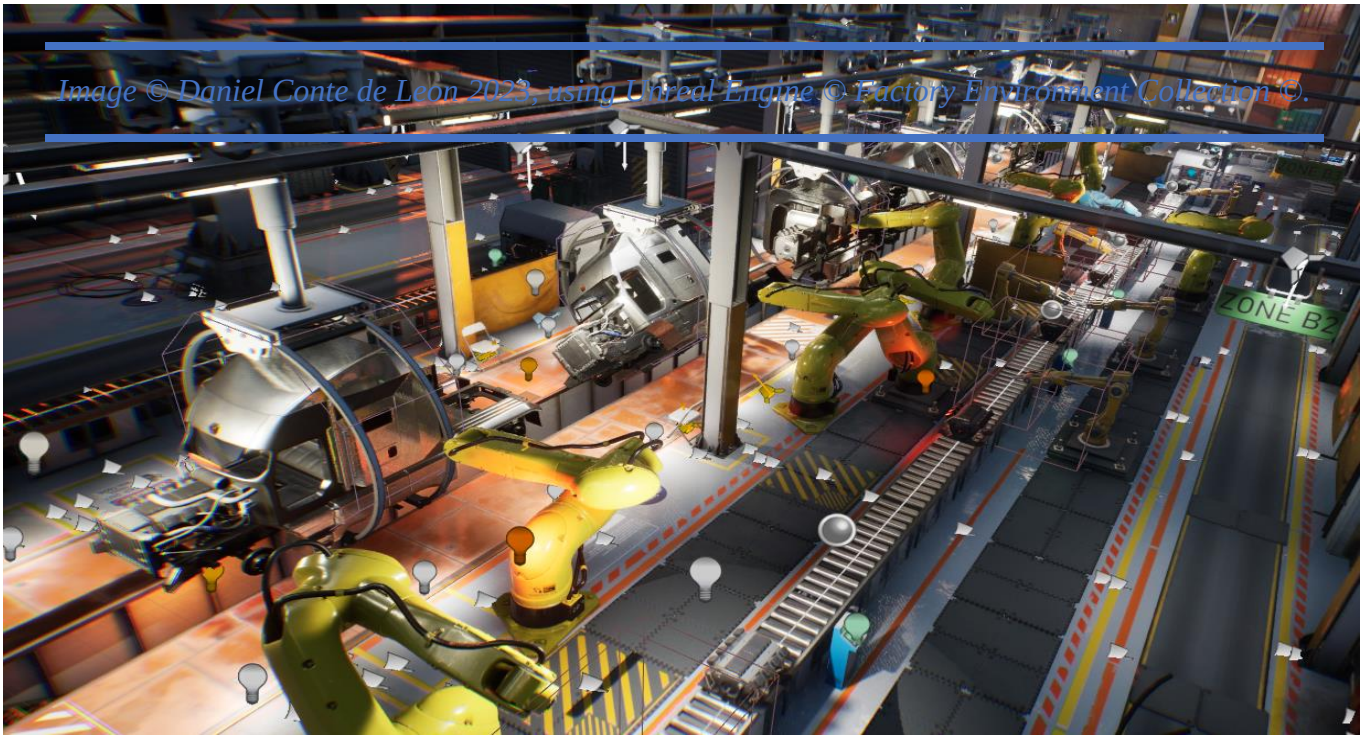

Image © Daniel Conte de Leon 2023, using Unreal Engine © Factory Environment Collection ©.