UNIVERSITEIT GENT
CAMPUS KORTRIJK

BUSINESS CASE 3

SIMULATION ATTACKS ON COMPLEX PRODUCTION NETWORKS USING DIGITAL SHADOW DEMONSTRATOR

Faculteit Ingenieurswetenschappen en Architectuur
Vakgroep EA18
IC4

Ing. Tinus Umans
Tinus.umans@ugent.be

www.ugent.be

1 DOCUMENT CONTROL AND REVIEW

Document check	
Author	**Tinus Umans**
Owner	**University Ghent**
Date created	**December 18, 2025**
Last revised by	**Tinus Umans**
Last revision date	**December 18, 2025**

1.1 Version management

Version	Date of approval	Approved by	Description of change
1.0	**December 18, 2025**	Tinus Umans	Draft of the Document

2 INTRO

In this document, we examine how a Digital Shadow, created in Visual Components, can be integrated with physical industrial controllers, to visualize cyberattacks. Without the risk of disrupting production. By connecting real hardware to a virtual environment, we demonstrate how cyber threats, targeting PLCs, can translate into real-world consequences. For this purpose, we created a fake tile producing factory, named Fictile. This will enhance both training and threat detection capabilities.

3 BUSINESS CASE

3.1 Problem

Showcasing the impact of a cyberattack has always been a difficult task. One of the best motivators to invest in cybersecurity is unfortunately still experiencing an attack. However, attacking a live production line presents risks in damaging expensive equipment, causing costly downtime, or even risking health and safety of employees. Furthermore, reading logs or network traffic (PCAP files) does not intuitively convey the severity of an attack to non-technical management.

3.2 Proposal

Implement a Digital Shadow of a fictive factory. This virtual factory will be driven by real-world PLCs (Siemens, Phoenix Contact and Beckhoff). When an attacker manipulates the real PLC code or traffic, the physical impact (conveyor belts, robotic arms, ovens overheating) is instantly visualized in the 3D simulation, without damaging real machinery.

3.3 Expected Benefits

- Safe “Red Teaming”: execute destructive attacks on real controllers without destroying physical assets
- Visualizing Impact: Translate abstract code changes into visible physical outcomes for stakeholders
- Multi-vendor interoperability: validate security across different hardware ecosystems (Siemens, Phoenix Contact, Beckhoff)
- Enhanced training: allows students and engineers to see the cause-and-effect relationship between network intrusion and physical process failures.

4 DEFINITIONS

4.1 Digital Shadow

A digital shadow is a one-way digital representation of a physical object or system. Unlike a digital twin (which often implies a bi-directional data flow where simulation can also control the physical equipment), the shadow receives real-time state data from the physical PLCs.

4.2 Visual Components

Visual Components is a leading 3D manufacturing simulation software. It allows users to design, simulate and visualize industrial processes. These can range from one small production line, to the logistical flow of a complete company. Crucially for this case, it features robust “Connectivity” plugins, that allows our 3D factory model to be driven by external signals (OPC UA, ADS, S7, …) from real PLCs.

5 REALISTIC ATTACK VECTORS & VULNERABILITIES

To ensure the Digital Shadow serves as an effective training and validation tool, the environment is intentionally configured to reflect common industrial realities - where legacy systems mix with modern technologies. We utilize specific, but realistic vulnerabilities to trigger the physical consequences observed in the simulation:

- Insecure Industrial Protocols (Cleartext Traffic)

We leverage the inherent lack of authentication in older communication protocols. Protocols like Modbus, S7 Communication Protocol (S7Comm) are widely used protocols, which can be mimicked with common tools like Snap7 or low difficulty Python scripts. These unsafe protocols allow attackers to inject malicious packets into industrial traffic, like overriding certain variables used in the PLC logic, all without needing a password.

- Outdated Firmware & Unpatched OS

A common industrial mindset is still “if it works, don’t touch it”, since any unnecessary downtime is costly. Devices like Beckhoff can run outdated Windows Embedded/IoT versions. This allows a scenario where the underlying OS is missing critical security patches. These vulnerabilities could be used to inject ransomware into the industrial network and can freeze or delay real-time logic, causing the digital shadow’s hydraulic press to miss a tile.

- Man-in-the-Middle (MITM) on unencrypted data transfers:

The Phoenix Contact printing process relies on downloading image files from a server to print onto tiles. We utilize unencrypted FTP or HTTP protocols for this transfer—a common oversight in OT environments. This setup allows us to demonstrate an ARP Spoofing attack where a hacker intercepts the file transfer and swaps the valid tile image for a corrupted one, instantly visualized in the simulation as the printer producing "defaced" product batches.

- Weak Authentication & Default Credentials

Many OT devices are deployed with default passwords to ensure easy maintenance by engineers. We replicate this by leaving the web-based management interfaces of some PLCs protected only by default credentials (e.g., admin/private or admin/1234). This highlights how easily an attacker can gain administrative control to stop the CPU or force a factory reset, triggering a total blackout in the virtual factory.

Not all real-life attack vectors are covered in this setup, that would be an enormous task. The decision was made to focus on the more low hanging fruits, like weak authentication, with more challenging scenarios for more advanced users.

To incentivize users, each vulnerability leads to a “Flag”. Each flag can be submitted to a local hosted website to gain points. This “Capture the Flag” has proven most effective in motivating users to find all vulnerabilities and navigate this industrial network safely.

6 IMPLEMENTATION: THE FICTILE FACTORY

Figure 1 Overview of Fictile Factory Digital Shadow

The digital shadow visualizes the complete lifecycle of a tile. The process is segmented into three distinct “cases", each controlled by a specific vendor's hardware. While multiple attack vectors are present in each case, only one example is given here.

6.1 Case 1 : Beckhoff - Raw Materials & Pressing

Figure 2 Overview Beckhoff Case

6.1.1 The Process

Raw powder is fed from a silo, moved via conveyor to a mold, and compressed into a tile shape by a hydraulic press.

6.1.2 Hardware Integration

- CX9020: Controls the hydraulic press. When a tile is detected, the press is activated .
- CX5230: Manages the mold filling. It ensures powder is distributed even before the press activates.

6.1.3 Potential Attack

The CX9020 uses (by default) cerHost. This allows an engineer to log onto the device and change settings as required. However, the software (provided by Microsoft and Beckhoff) uses a client-side authentication. An attacker can easily bypass this and thus gain access without even needing a password.
After this, a user could download the source code and change some small functionality.

- Visual Components

Tiles are not pressed anymore. While the line still seems to work at a quick glance, no tiles are made under the hydraulic press.

6.2 Case 2: Phoenix Contact – Surface Treatment & Color

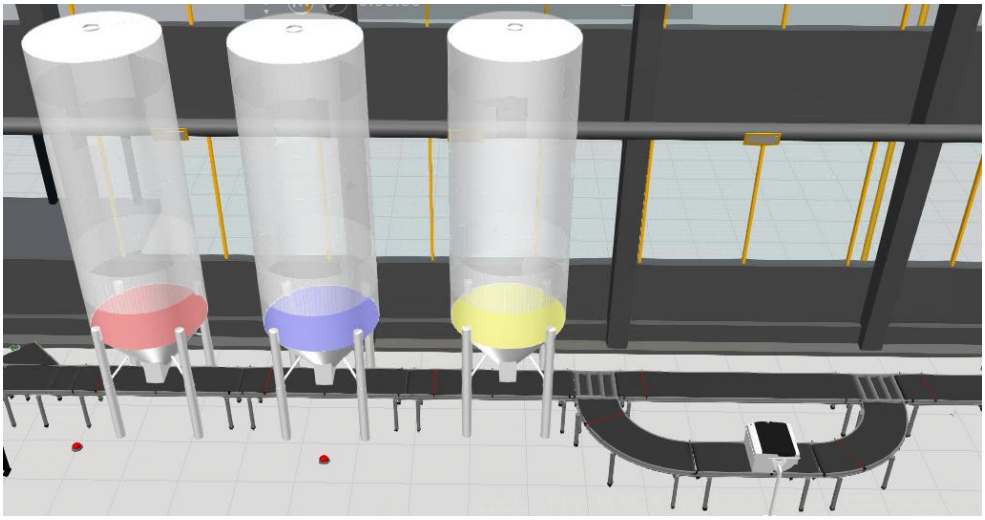

Figure 3 Overview Phoenix Contact Case

6.2.1 The Process

The pressed tile moves to the coloring station. Ink tanks (Red, Blue, Yellow) supply a mixing roller. A smart inkjet printer then applies a specific design based on ERP data.

6.2.2 Hardware integration

- ILC 390 PN: Manages the ink logistics. It triggers pumps when ink buffers are low and controls the mixing valves.
- ILC 151 Eth: controls the conveyor belts for this line.
- AXC F 2151 (PLCnext): This Linux-based controller handles the high-level logic, downloading specific image files from an internal server to print onto the tile.

6.2.3 Potential Attack

ILC390 and ILC151 still use an old phoenix contact protocol, which allows attackers to enumerate, read and write variables in the plc. An attacker could use this to overwrite the Paint Boolean, thus draining the paint from the reservoir, without any tile present. This results in a big capital loss for the company, since paint is drained, but no tiles are colored.

- Visual Components

One or more reservoirs for paint is constantly empty. When dropping below a certain level, the paint is automatically refilled, but this carries an overall cost for the company.

6.3 Case 3 : Siemens – Baking

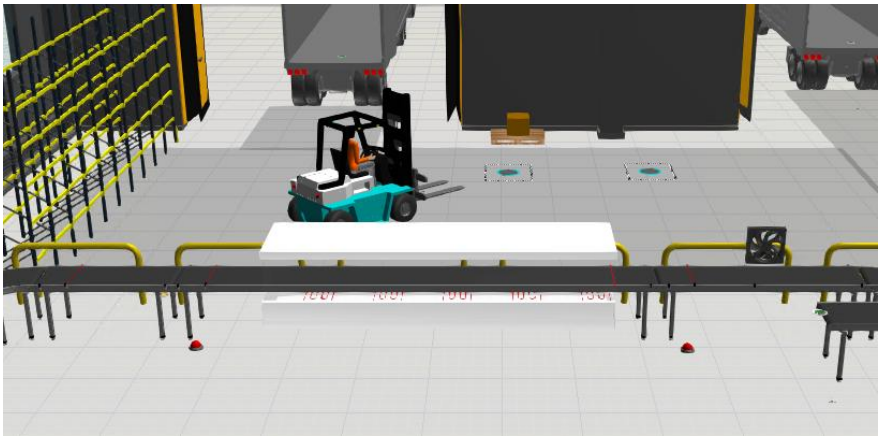

Figure 4 Overview Siemens Case

6.3.1 The process

The painted tiles enter a high-temperature oven. After baking, they are cooled, labeled and stacked by an XY robot.

6.3.2 Hardware integration

- S7-1500 : Controls the burner "Flames" and temperature regulation. It creates the critical "Heat Tower" logic.
- S7-1200 : Controls the conveyors of this line.

6.3.3 Potential Attack

An attacker can levy the modbus vulnerability (or S7comm) to overwrite the “flames” of the oven, thus increasing the temperature of the oven. When the temperature gets too high, the tiles will “burn” black, instead of baking.

- Visual Components

The tiles normally exit the oven with a pink color, indicating a finished product. But when the temperature is too high they exit it black. The packaging robot is not equipped with a camera to check for defects, thus a burned tile is packaged and sent to a customer.

7 FACTORY SOFTWARE

In a standard production environment, the process would be orchestrated by a commercial Enterprise Resource Planning (ERP) system (e.g., SAP, Odoo).

However, for the scope of this Digital Shadow, deploying a full-scale commercial ERP was deemed inefficient due to prohibitive licensing costs and the disproportionate configuration effort required compared to the educational value added.
Instead, we opted to develop a proprietary, lightweight management suite tailored specifically for this use case. This custom-built application functions as a simplified "ERP". Integrating a user-friendly Web Shop for placing tile orders, a Warehouse Management System (WMS) for tracking inventory, and a Manufacturing Execution System (MES) to translate orders into PLC instructions. This approach reduces complexity and allows us to summarize the cost of an attack with ease.

The landscape of commercial ERP systems (e.g., SAP, Microsoft Dynamics, Odoo) is highly fragmented, with each platform possessing unique architectures and vulnerabilities. Developing complex exploits for a specific ERP interface would consume significant resources without providing transferable knowledge for the majority of stakeholders.

Instead, our mission focuses strictly on Operational Technology (OT) risks.

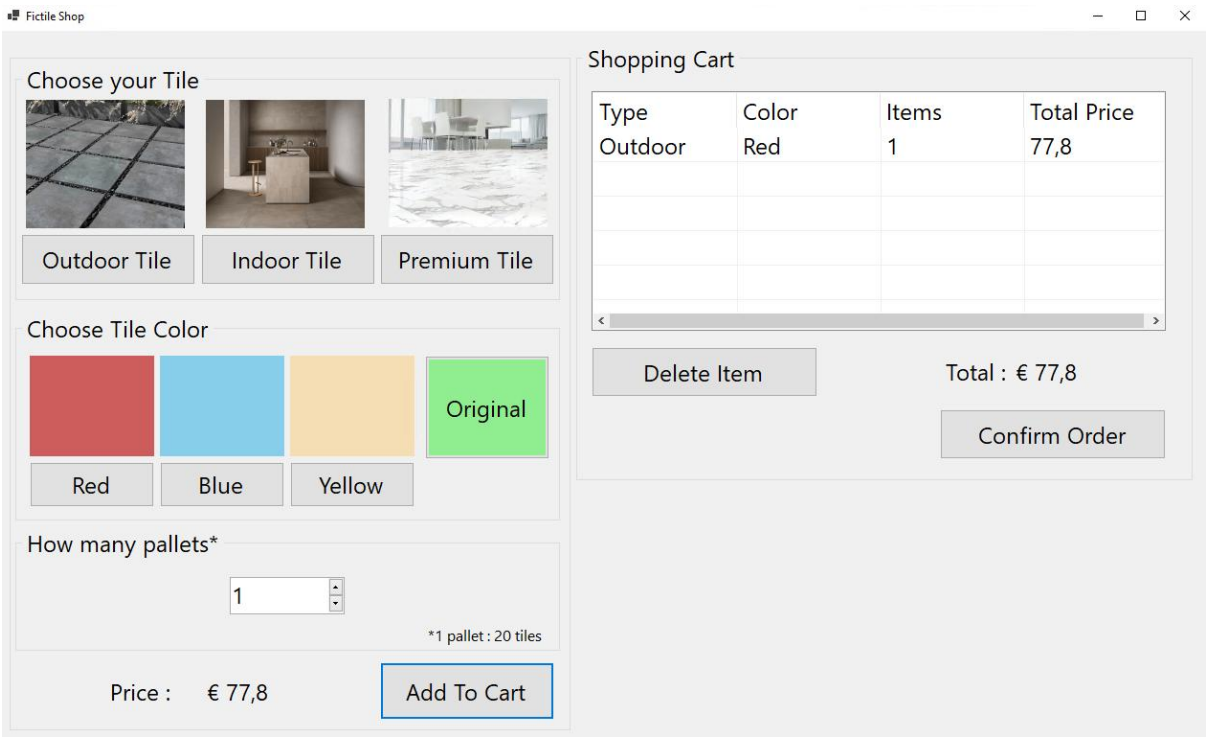

Figure 5 Overview Fictile Shop UI

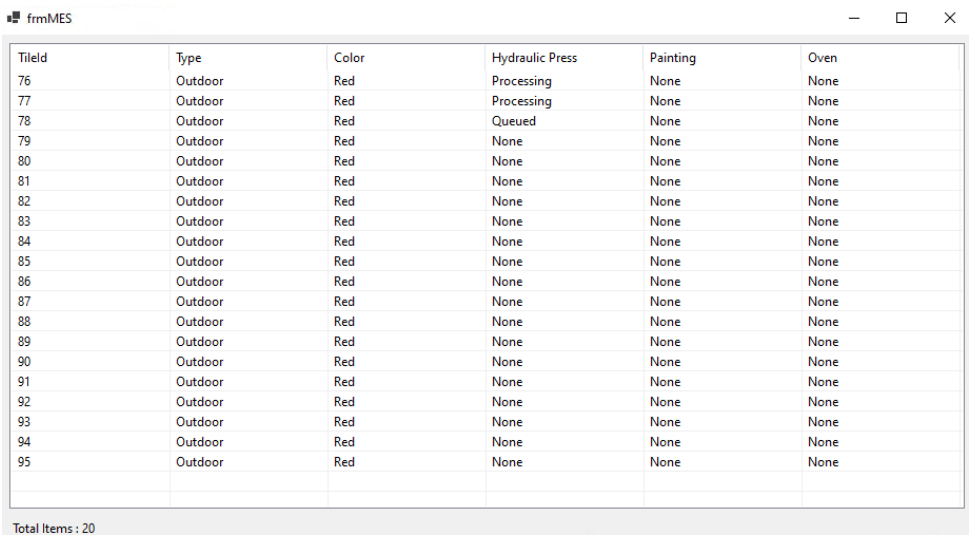

Figure 6 Overview Current MES orders

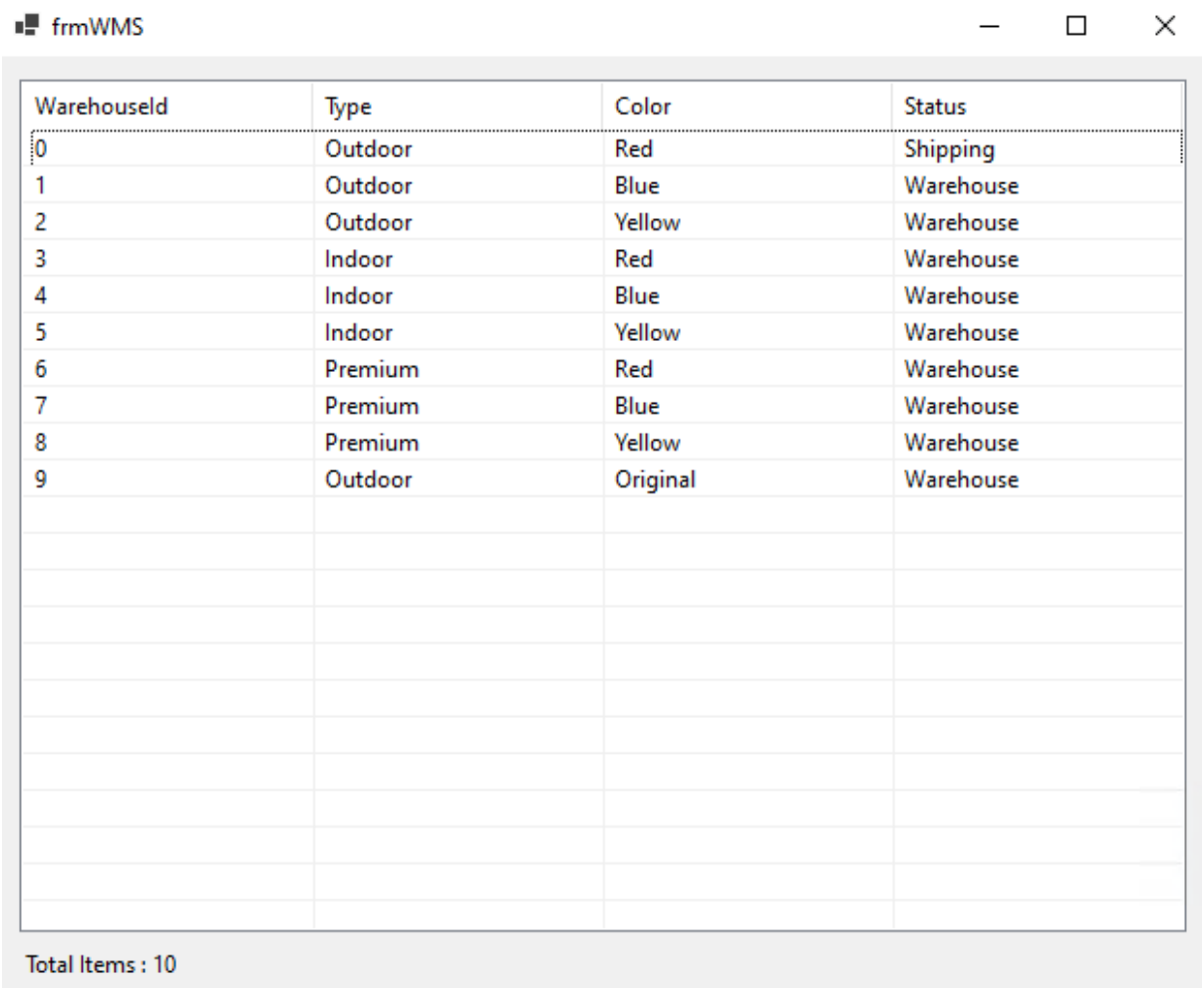

Figure 7 Overview Warehouse Management System

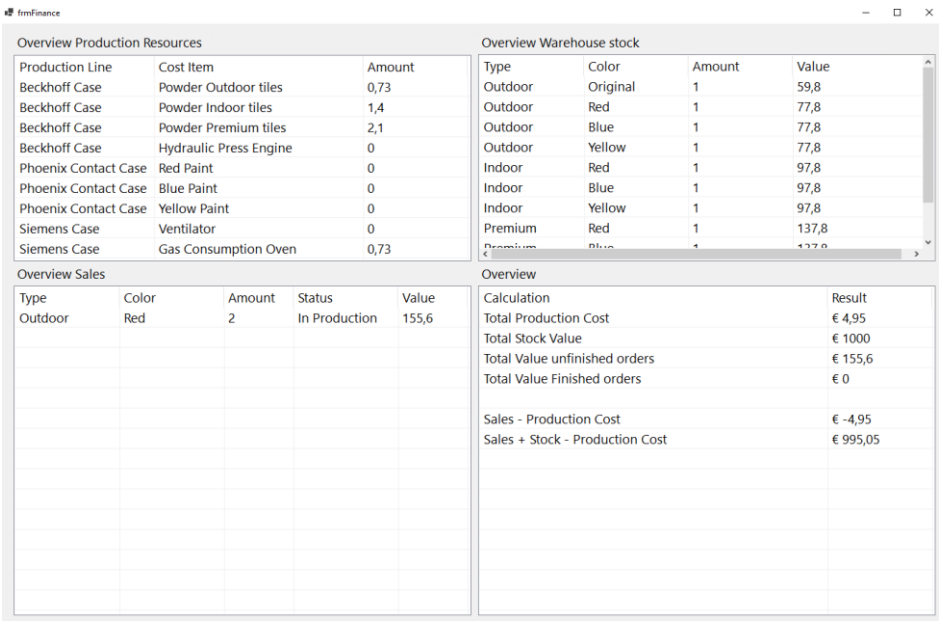

Figure 8 Overview Financial situation Fictile

8 RECOMMENDATION

8.1 Risks

- Interference with Simulation-Specific Traffic

The architecture relies on a specific data stream to synchronize the physical PLCs with Visual Components. In a real-world scenario, this traffic would not exist. There is a risk that a red-teamer or attacker may inadvertently or intentionally target this simulation synchronization traffic rather than the actual industrial control protocols. Tampering with this link will desynchronize or break the visualization tool, resulting in a "false positive" that disrupts the demonstration without exposing a genuine vulnerability in the industrial hardware or logic.

- Limitations of Physics Fidelity:

While the Digital Shadow provides a powerful visual representation of cyber-physical attacks, the simulation engine has constraints regarding fluid dynamics and destructive physics. The visualization focuses on operational impact—such as machine collisions, line stoppages, and conveyor jams—rather than cinematic destruction. Stakeholders should manage expectations: catastrophic failures like exploding pressure vessels or fluid spills spreading across the factory floor are abstracted and indicated by system alarms or basic animations, rather than photorealistic physics.

8.2 Value

- Bridge the IT/OT Gap

This solution provides the perfect visual tool to explain OT security to IT professionals. IT staff understand code; they do not always understand the real-life consequences.

- Zero-Downtime Resilience Testing (ROI)

Traditional security testing on live production lines requires scheduled downtime, costing the company revenue and risking physical asset damage. This solution offers a risk-free simulation environment. We can stress-test our resilience against catastrophic cyber-events—and validate our recovery procedures—without pausing operations or risking a single Euro in equipment damage.

- Regulatory Assurance & Brand Protection (NIS2 / IEC 62443)

With the enforcement of the NIS2 directive and strict IEC 62443 standards, verifying network segmentation is a legal and financial necessity. This platform provides auditable proof that our critical "Control Networks" are adequately isolated from the "Corporate Network," demonstrating due diligence to auditors and protecting the company from liability and reputational damage.