Norwegian Centre for Research-based Innovation

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

# Enhancing Threat Modeling in Manufacturing with Digital Twin Technology

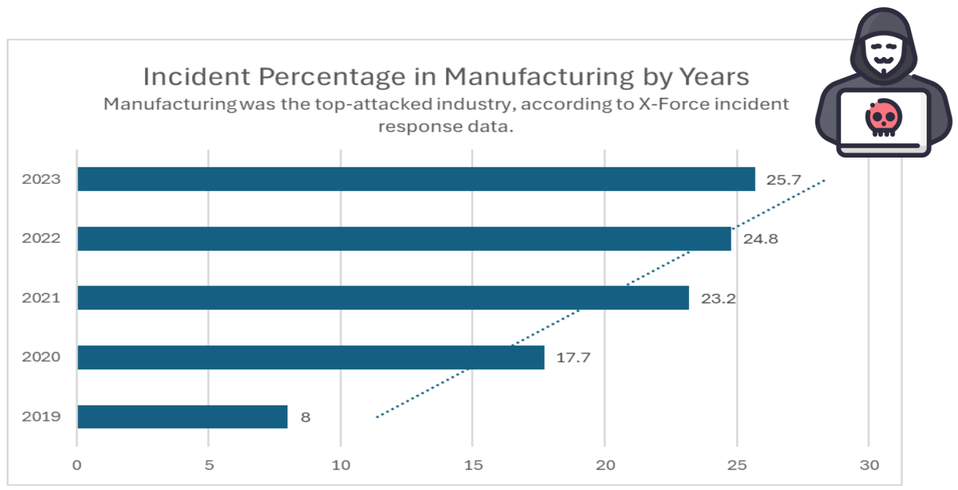
The manufacturing sector is witnessing an increasing frequency of cyberattacks, largely driven by the integration of Industry 4.0 technologies such as IoT, cloud computing, and digital twins. These advancements have significantly expanded the attack surface of Industrial Control Systems (ICS), rendering traditional cybersecurity measures inadequate. There is a critical need for proactive cybersecurity approaches that provide strong protection while ensuring continuity of operations in production environments.

## Objectives

In our study, we propose the use of Digital Twin technology to enhance threat modeling.

**Objectives:**

- To develop an optimized threat modeling framework using digital twin for data collection, monitoring, replication, analysis, and simulation.
- To explore machine learning's role in predictive analysis for cyber threat identification.



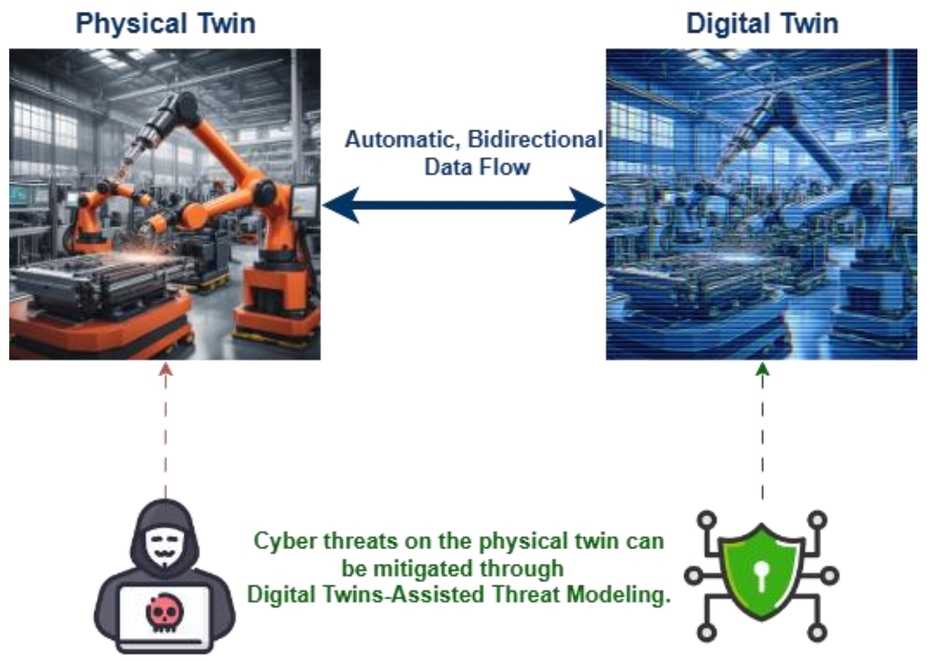

IBM Security X-Force Threat Intelligence Index 2024 (2023) Retrieved from https://www.ibm.com/reports/threat-intelligence

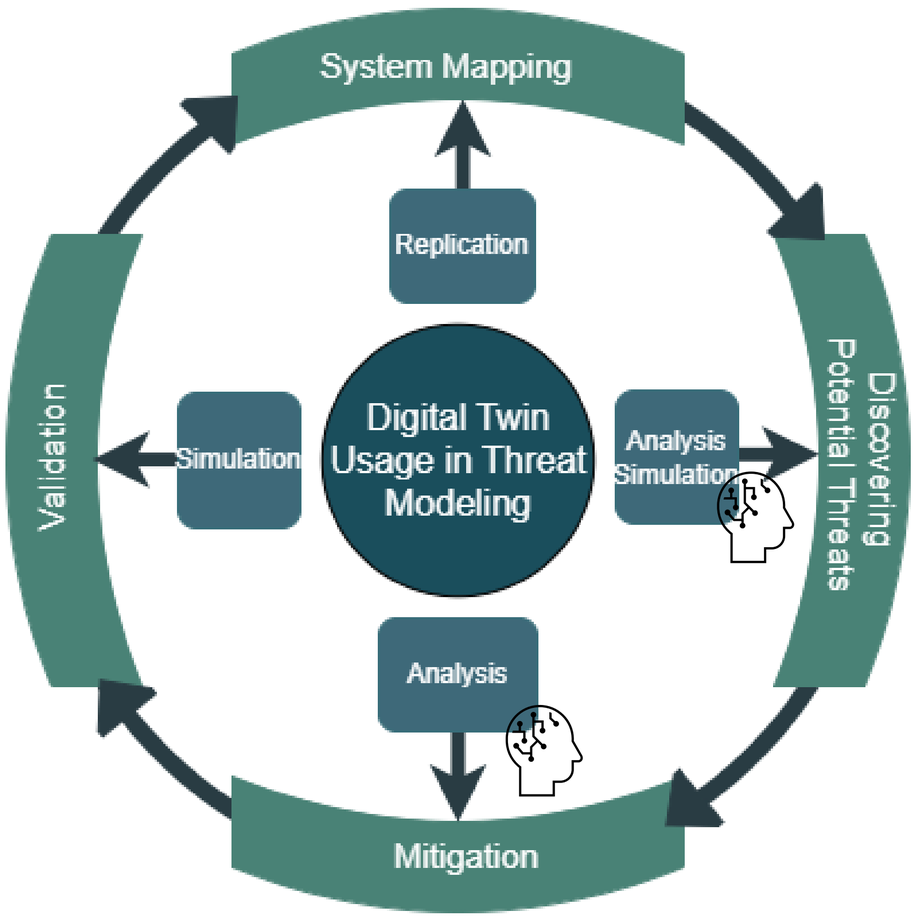
## Methodology

**Threat Modeling:** Threat modeling techniques will be applied to identify vulnerabilities in the system, focusing on key stages like system mapping, discovering potential threats, and mitigation and validation.

**Digital Twin Technology:** A virtual representation of physical assets allows real-time data collection, monitoring, replication, analysis and simulation of potential threats without disrupting ongoing production.

**Machine Learning:** Machine learning algorithms will process data collected through the digital twin to identify patterns, predict potential threats, and improve decision-making. This predictive capability enhances the system's ability to anticipate potential cyber threats and take mitigation actions.



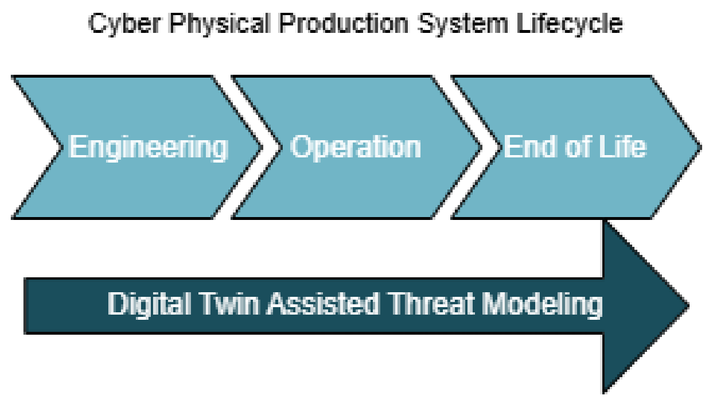

## Expected Results

**Situational Awareness:** The integration of Digital Twin and machine learning will enhance situational awareness by providing real-time insights into the security status of ICS.

**Continuity:** The proposed framework will safeguard operational continuity without disrupting production. The threat model can be applied at every stage of the life cycle.

**Dynamicity:** The system will be capable of adapting to the constantly changing dynamics of the manufacturing environment. As new threats and system configurations emerge, the threat model will evolve to maintain a robust security posture that addresses current and future challenges.

**Automation:** The use of machine learning and Digital Twin technology will automation. This automation enhances efficiency, reduces human error, and speeds up decision-making processes in identifying and mitigating cyber threats.




**PhD Candidate**: Gizem Erceylan
**Supervisors:** Vasileios Gkioulos, Sokratis Katsikas, Aida Akbarzadeh, Sandeep Pirbhulal