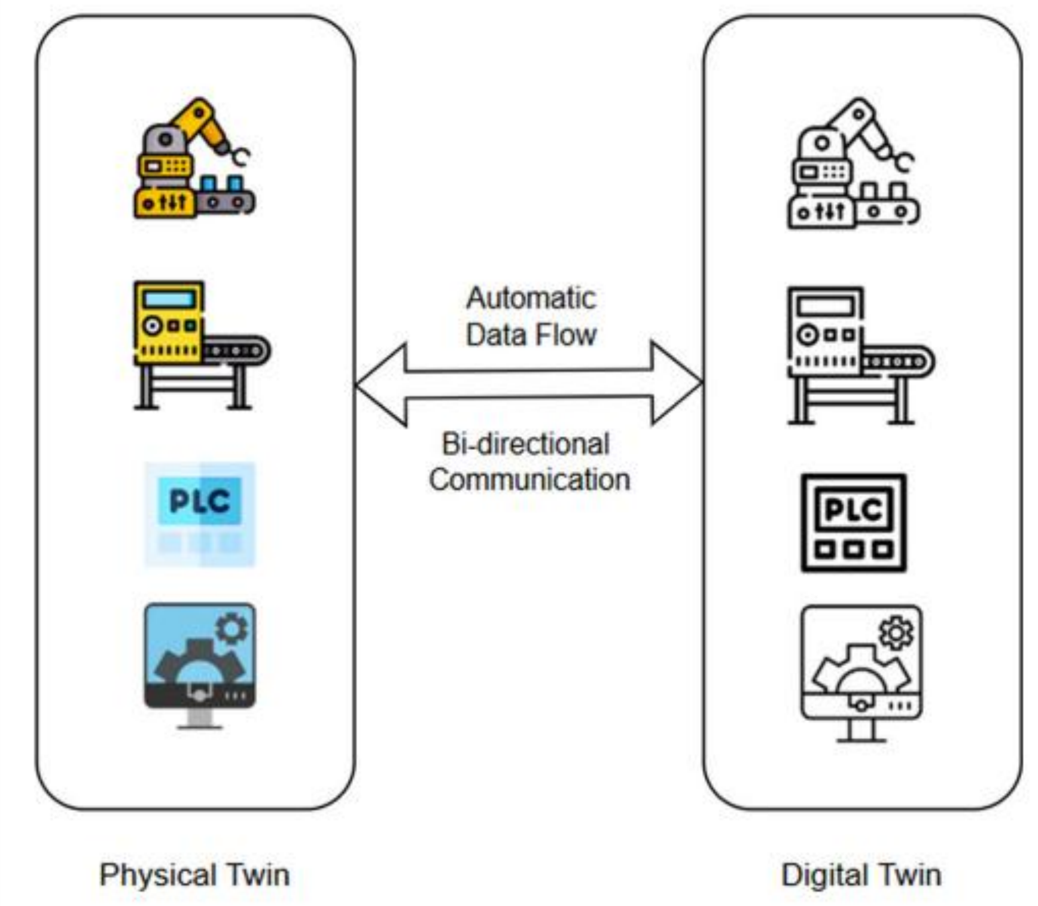
Norwegian Centre for Research-based Innovation

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Digital Twin-Assisted Threat Modeling Framework for ICS Cybersecurity

Industrial Control Systems (ICS) form the backbone of critical infrastructure, where uninterrupted availability and production continuity are vital. However, these systems are increasingly vulnerable to complex and multi-stage cyberattacks, particularly Advanced Persistent Threats (APTs). Traditional, static threat modeling approaches fail to address the dynamic and operational nature of ICS/CPS environments and the sophistication of modern attacks. To overcome these challenges, this study introduces a Digital Twin–assisted Threat Modeling (DT-TM) framework to enhance ICS cybersecurity.



Digital Twin Communication and Data Flow

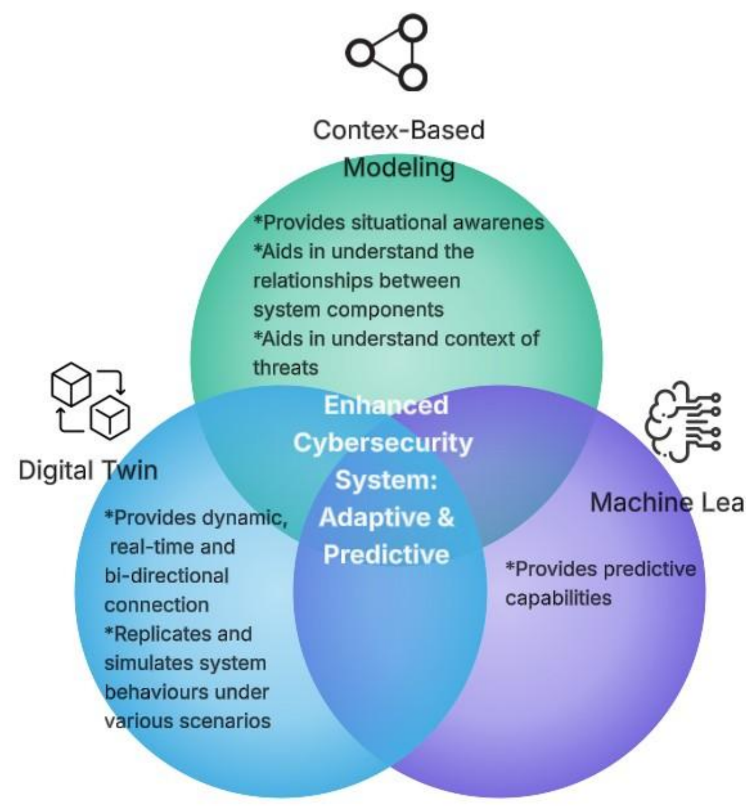
Digital Twin-Assisted Threat Modeling (DT-TM) Benefits

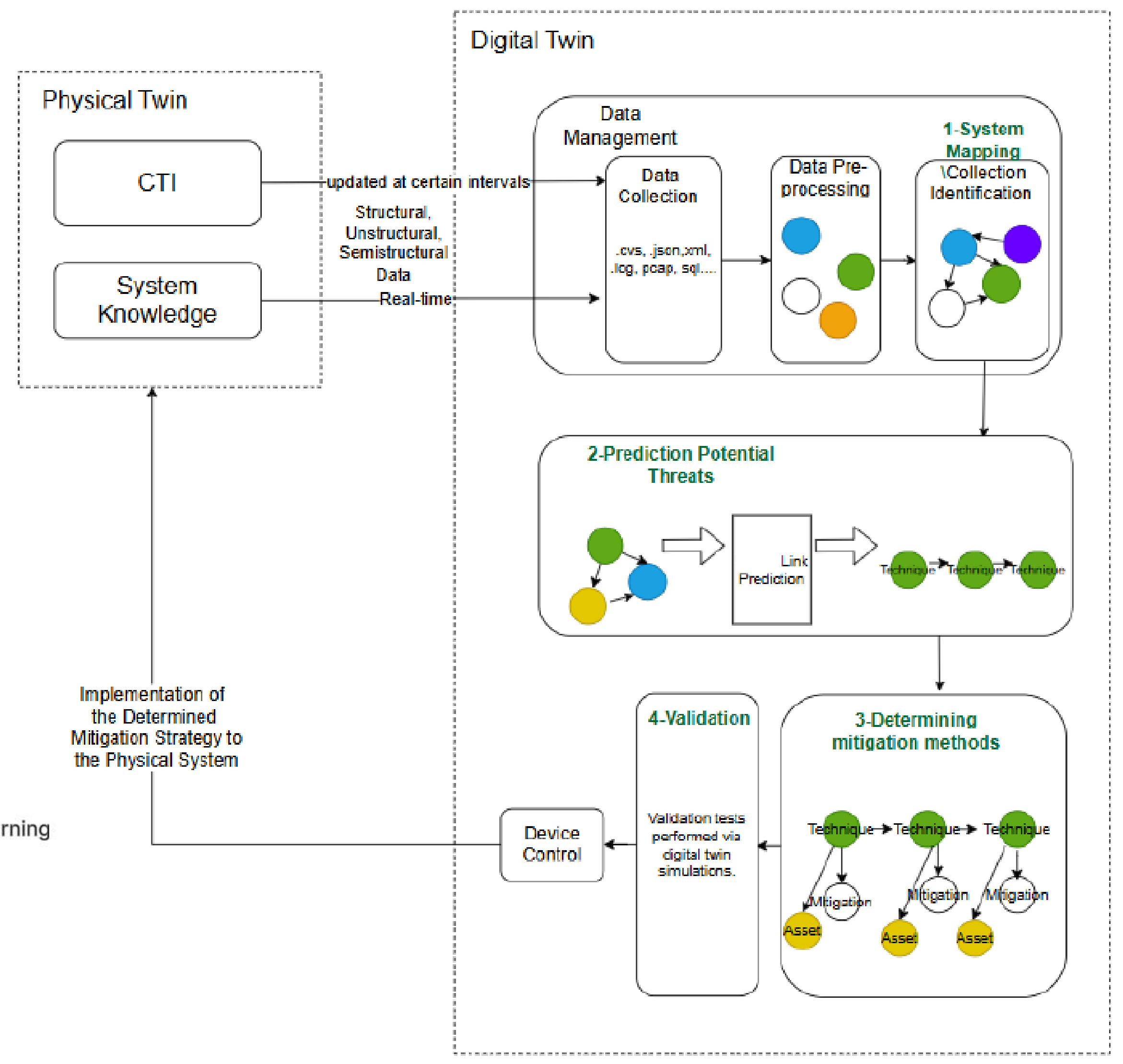
DT-TM transforms traditional cybersecurity approaches by enabling continuous, dynamic, and autonomous threat analysis across the entire system lifecycle. Through real-time data integration and enhanced situational awareness, it supports proactive detection and mitigation of evolving threats. By combining Cyber Threat Intelligence (CTI) with system-specific data, digital twins ensure that threat models remain accurate, adaptive, and up to date. This approach strengthens cyber resilience, improves prediction and response capabilities.

ICS Threat Model Requirements	Conventional Threat Models	Digital Twin-Assisted Threat Models
Should be applied throughout the entire system life-cycle, not just during the design phase.	✗ Partial life-cycle	✓ Entire life-cycle (Continuous)
Should be dynamic to continuously assess vulnerabilities and create a security strategy that includes the most current threats.	✗ Static model	✓ Real-time adaptation (Dynamic)
Should be autonomous so that it can dynamically adapt, making them faster and reducing human error.	✗ Manual, time-consuming	✓ Autonomous, faster
Should have high level situational awareness to proactively prevent attacks.	✗ Limited system insight	✓ High level of situational awareness
Should have comprehensive threat intelligence since ICS systems contain many different components.	✗ Limited scope of threats	✓ Comprehensive threat intelligence
Should have strong analytical computing capability to predict sophisticated and constantly evolving cyber threats.	✗ Expert dependent	✓ Behavioral analytics

Prediction of Potential Threats

Potential cyber threats are predicted using a digital twin–enabled knowledge graph that continuously integrates real-time system data and CTI. A neural network model analyzes their relationships to infer likely attack paths and predict the next steps of potential attackers. These predictions enhance situational awareness and enable proactive defense through simulated threat scenarios and validation within the digital twin environment.

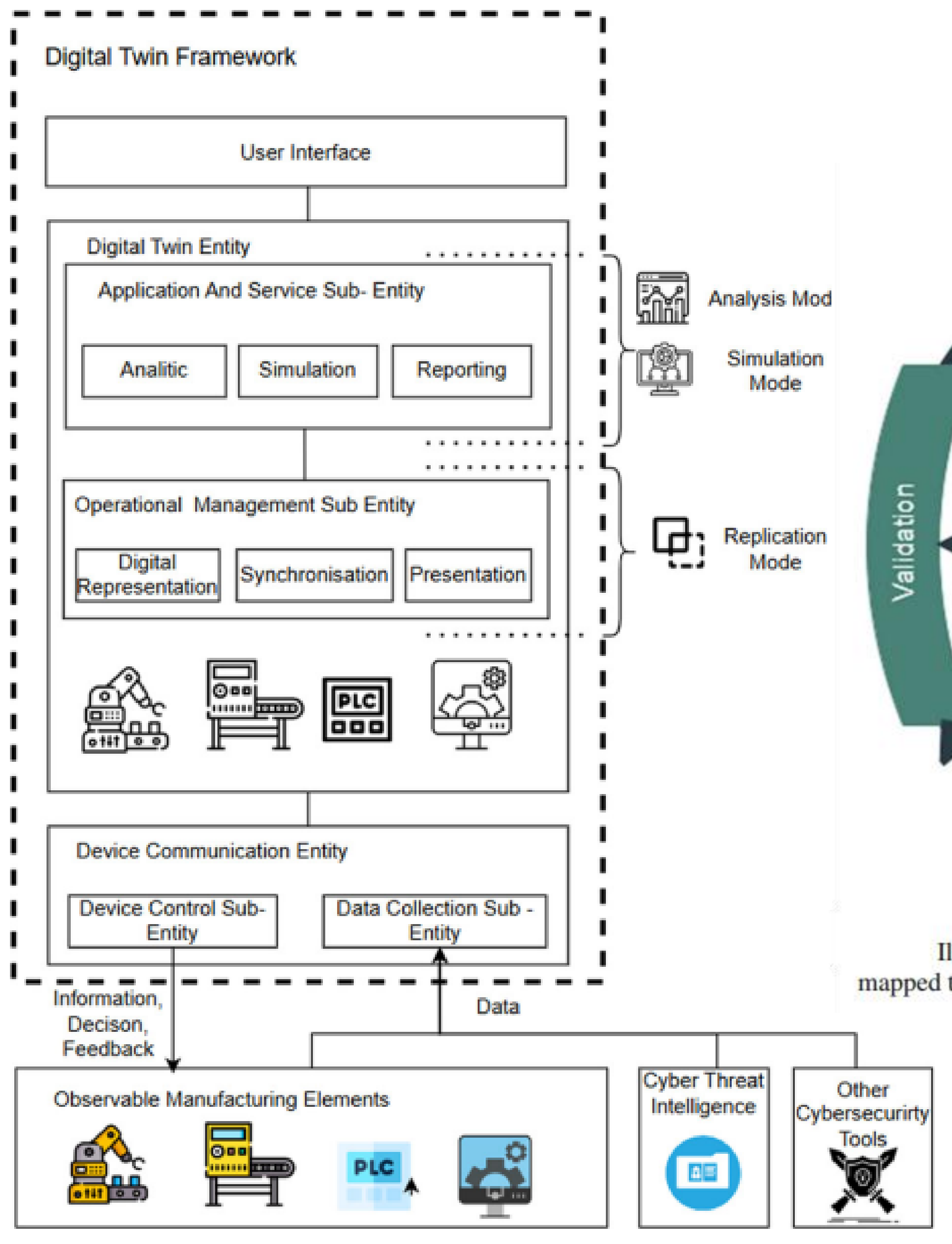

Contex-Based
Modeling
*Provides situational awarenes
*Aids in understand the relationships between system components
*Aids in understand context of threats
Enhanced Cybersecurity System: Adaptive & Predictive
Digital Twin
*Provides dynamic, real-time and bi-directional connection
*Replicates and simulates system behaviours under various scenarios
Machine Learning
*Provides predictive capabilities


Digital Twin
Physical Twin
CTI
System Knowledge
updated at certain intervals
Structural, Unstructural, Semistructural Data
Real-time
Data Management
Data Collection
.cvs, .json,xml, .log, pcap, sql....
Data Pre-processing
1-System Mapping \Collection Identification
2-Prediction Potential Threats
Link Prediction
Technique
Technique
Technique
3-Determining mitigation methods
Technique
Technique
Technique
Mitigation
Mitigation
Mitigation
Asset
Asset
Asset
4-Validation
Validation tests performed via digital twin simulations.
Device Control
Implementation of the Determined Mitigation Strategy to the Physical System

Suggested digital twin- assisted threat modeling structure

Digital Twin Integration into Threat Modeling

Integrating digital twin technology into threat modeling provides a data-driven, continuously updated representation of physical systems. Through its core operational modes—replication, simulation, and analysis—the digital twin enables accurate system mapping, proactive threat discovery, and effective validation of mitigation strategies without disrupting real operations. By aligning with frameworks such as ISO 23247 and leveraging insights from ECSO's digital twin proposals, this approach transforms static models into a continuous, intelligent, and lifecycle-spanning security process.


Digital Twin Framework
User Interface
Digital Twin Entity
Application And Service Sub- Entity
Analitic
Simulation
Reporting
Operational Management Sub Entity
Digital Representation
Synchronisation
Presentation
PLC
Analysis Mod
Simulation Mode
Replication Mode
Device Communication Entity
Device Control Sub-Entity
Data Collection Sub - Entity
Information, Decison, Feedback
Data
Observable Manufacturing Elements
PLC
Cyber Threat Intelligence
Other Cybersecurirty Tools

Adaptation of a digital twin-assissted threat modeling framework based on ISO 23247 with distinct operational modes

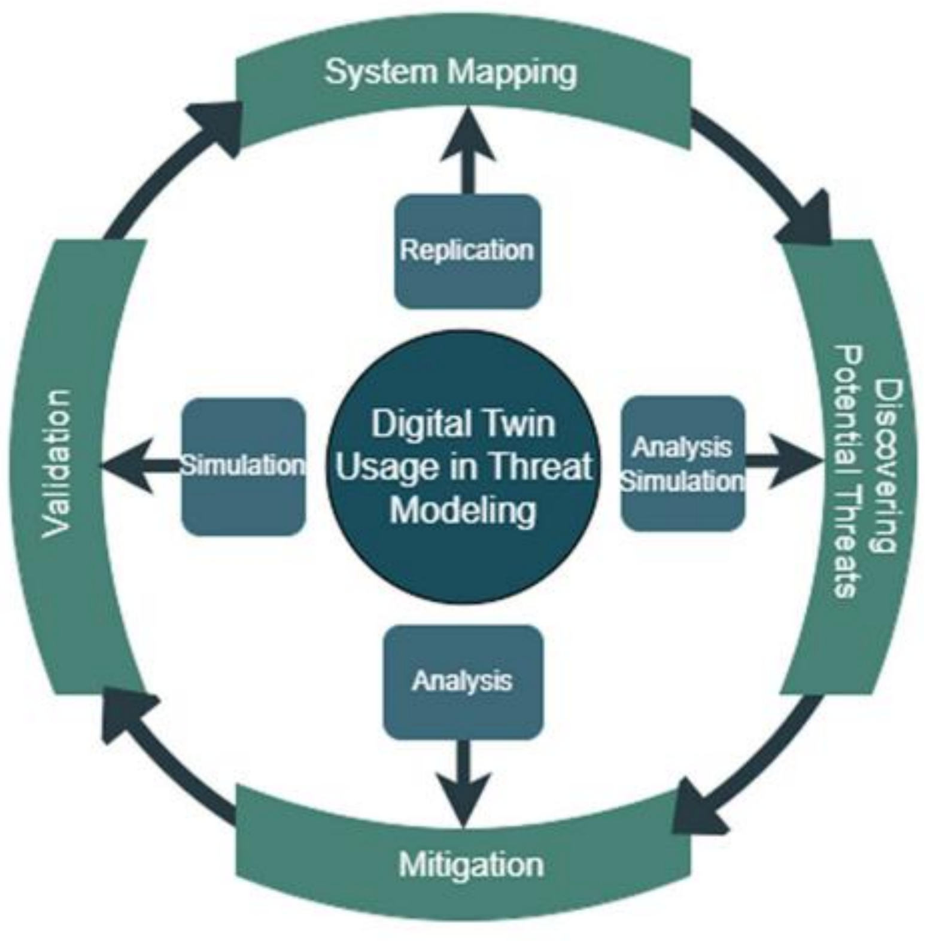
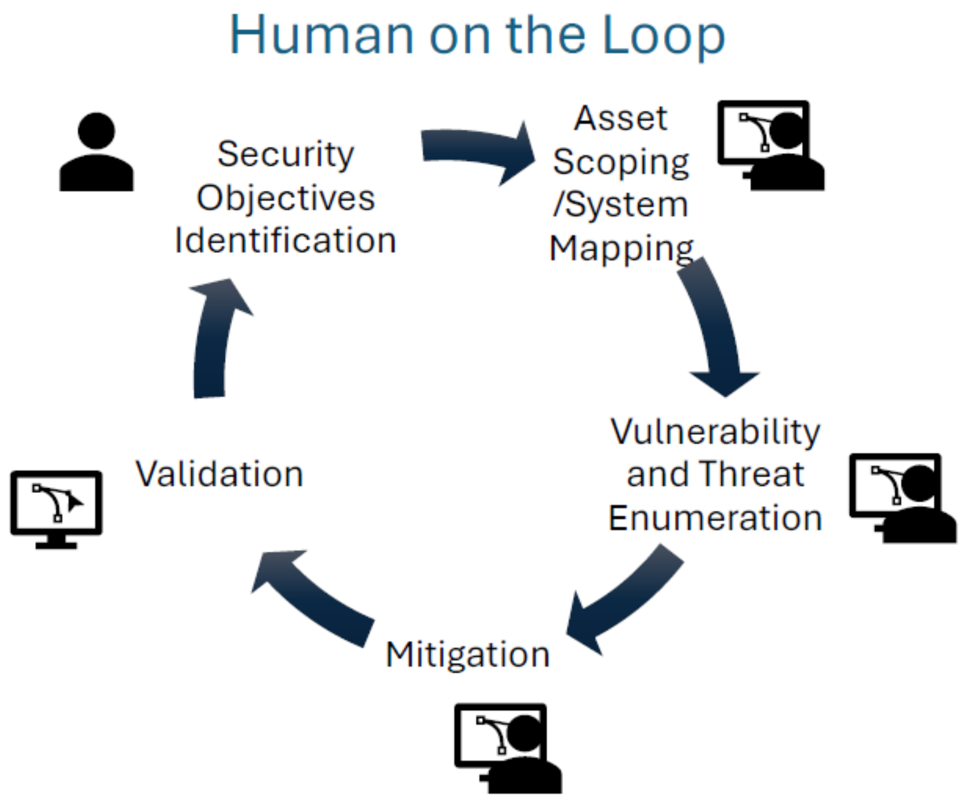


Illustration of different mode of the digital twin (inner circle) mapped to the four basic stages of threat modeling (outer circle)

Human-on-the-Loop Approach in Threat Modeling

The human-on-the-loop approach combines automation with expert oversight to achieve a balanced, adaptive, and cyber-resilient threat modeling process. While automation ensures rapid analysis and continuous monitoring, human experts provide contextual understanding and judgment in complex or unforeseen situations. This synergy enhances robustness, redundancy, and responsiveness—key pillars of cyber resilience—while maintaining transparency and adaptability across all stages of threat modeling.


Human on the Loop
Security Objectives Identification
Asset Scoping /System Mapping
Vulnerability and Threat Enumeration
Mitigation
Validation

PhD Candidate: Gizem Erceylan
Supervisors: Vasileios Gkioulos, Aida Akbarzadeh, Sokratis Katsikas, Sandeep Pirbhulal
www.ntnu.edu/norcics

NTNU Norwegian University of Science and Technology