CBIPS
Infrastructure Interdependencies

2026/02/25 Zoe Shih

Cybersecurity Risks and Defense Strategies in Digital-Twin–Enabled Smart Infrastructure: A Systematic Review

Emma Junior Emmanuel
13-11-2025

DT-Enabled Infrastructure

- Digital Twins (DTs) act as digital replicas of physical assets, fusing live telemetry with computational models to support closed-loop control.
- Applied across smart-infrastructure sectors including power systems, transportation, water, and industrial facilities
- The Tight Coupling: DTs collapse separate data and control paths into a single, time-sensitive pipeline: Data → Model/Sync → Actuation.
- Risk Propagation: Because of this integration, corruption at any stage (e.g., a sensor or a model) can propagate into physical operational decisions, affecting safety and reliability

Cybersecurity Risks

- Ingest & Model Risks: Telemetry poisoning and model drift can push the twin away from reality, leading to incorrect state inferences.
- Actuation Risks: Spoofed commands or unsafe set-points can bypass operator safeguards and push malicious instructions directly to the physical plant

Resilience Frameworks

- Implementation of IEC 62443 (Zones and Conduits) to segment systems and NIST SP 800-82 for OT-aware safeguards.
- Technical Controls: Ensuring end-to-end data trust through signed telemetry, mTLS, command signing, and independent out-of-band safety interlocks
- Safety Sandbox: DTs allow operators to rehearse incidents, test detection rules, and validate response playbooks without risking the actual physical system

Agent-Based Modelling of High-Speed Railway (HSR) Interdependent Critical Infrastructures

Pattrapon Kongsap and Sakdirat Kaewunruen
06 February 2024

High-Speed Railway

- HSR is a catalyst for economic growth but operates through highly complex, interdependent networks
- The Resilience Challenge: Disruptions are no longer local; a failure in one node (e.g., signaling in one city) can affect cross-border interconnected services (e.g., London-Paris-Brussels)
- Coupled Domains: HSR resilience depends on the interaction between physical infrastructure (tracks/trains), power supply, telecommunications, staff management, and passenger behavior
- Chain Reactions: Internal factors (equipment failure) or external factors (strikes, weather) can trigger service cancellations and massive economic losses

Physical and Cyber Threat

- Cyber Threats: Growing concern over DoS attacks targeting Operational Technology (OT) and the challenges of IT/OT convergence.
- Holistic Strategy: Resilience requires a strategy that treats cyber and physical hazards as an integrated threat to operational integrity

Agent-Based Modeling (ABM) for Resilience

- Unlike mathematical models, ABM captures emergent incidents and describes natural system interactions with high flexibility
- Modeling Agents: Defining passengers, train agents, stations, and railroads as distinct agents to simulate behavior under stress
- Big Data Integration: Using real-world data (AFC, CCTV, GPS) to calibrate ABMs for accurate passenger behavior prediction during disruptions.
- Multi-Agent Systems: Developing adaptive models to identify "critical agents" that most impact system performance under unforeseen threats

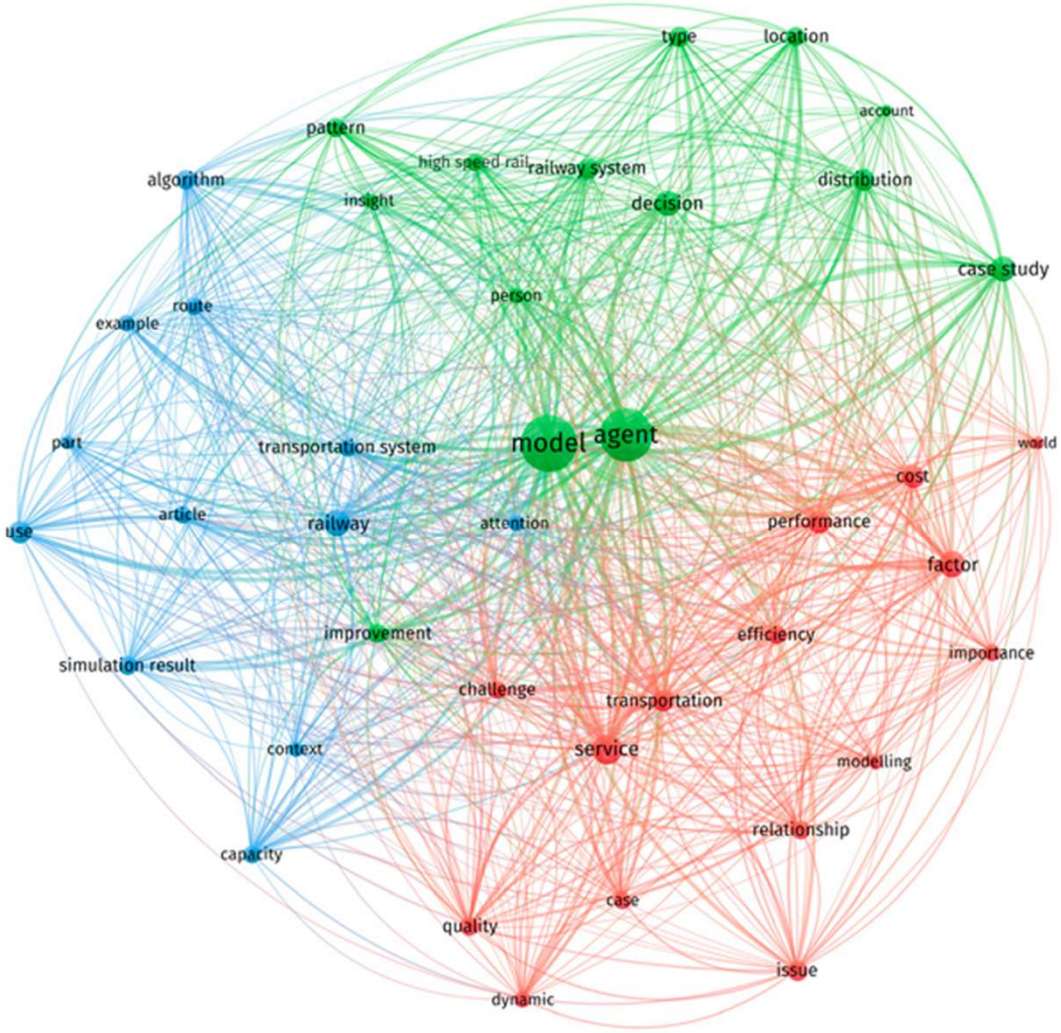


FIGURE 4
Overview clusters of the network maps, demonstrating the contour of density of ABM research targets and aims.

•**Disruption Scenario Simulation:** Agent-Based Modeling (ABM) can be used to simulate high-speed rail (HSR) operations when facing physical threats (e.g., natural disasters, strikes, power outages) or cyber threats (e.g., DoS attacks, OT system tampering).

•**Passenger Behavior Prediction:** ABM can analyze how individual passengers respond to train delays or service cancellations, enabling operators to test evacuation plans or real-time dispatch strategies without disrupting the real-world system.

•**System Resilience Enhancement:** By integrating real-world data sources (e.g., AFC automated fare collection, CCTV surveillance, GPS tracking), ABM enables more accurate simulations. It helps identify “critical agents” that significantly influence system performance, thereby strengthening overall safety and resilience.

Cyber-Physical Cascading Failure and Resilience of Power Grid

Md Zahidul Islam

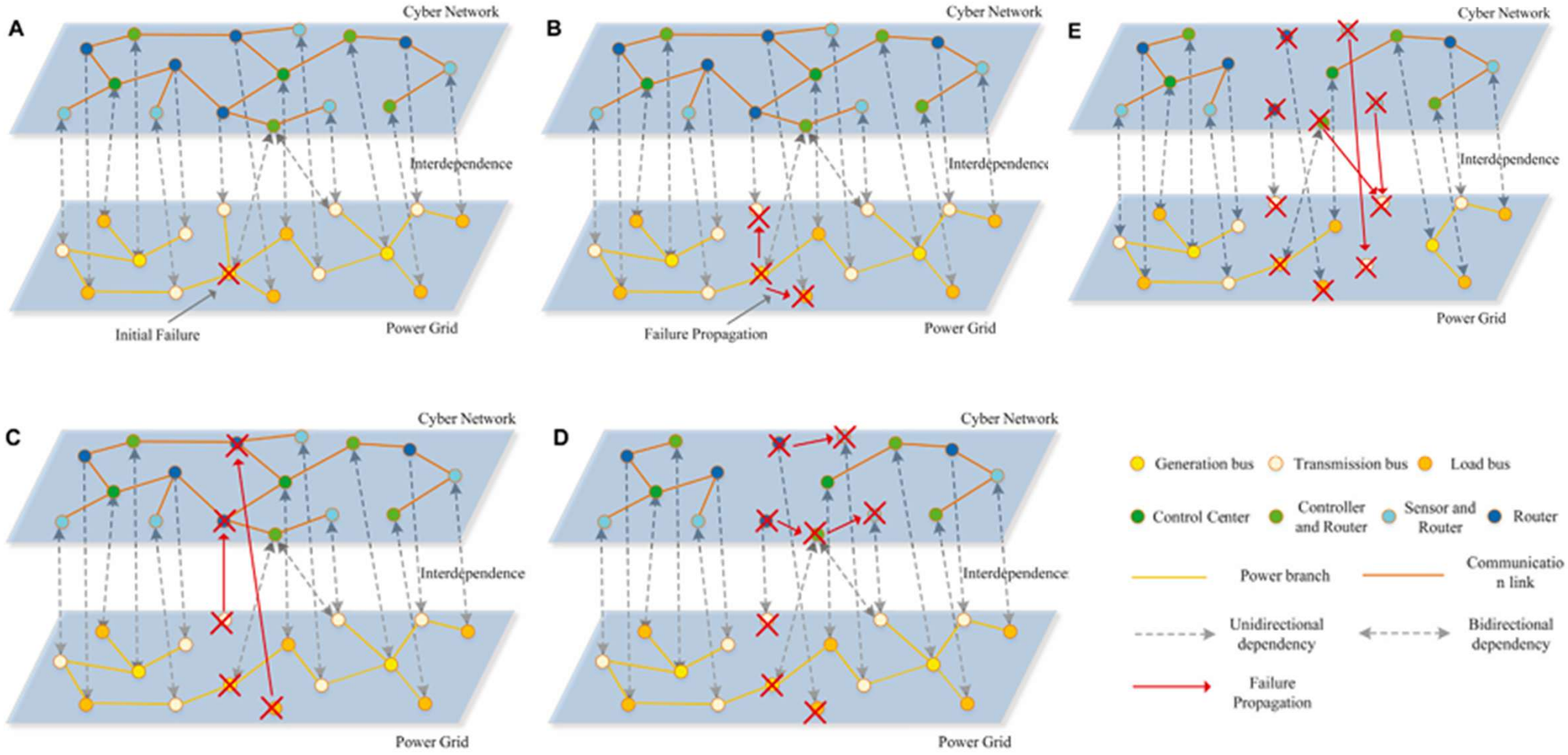
09 February 2023

Cyber-Physical Power Systems

- Modern grids integrate physical power delivery with sensors, advanced communication, and computing resources
- While this enables "smart" monitoring, it introduces new vulnerabilities and complex failure mechanisms
- The power grid depends on the cyber network for control/monitoring
- The cyber network depends on the grid for energy
- A small malfunction in one network can disable nodes in the other, leading to a large-scale, seemingly unexpected collapse (e.g., 2003 Italy Blackout)

Failures

- Intra-Domain: Failures within the same network (e.g., power line overload, data congestion).
- Inter-Domain: Failure propagating across networks (e.g., a power outage causing a router to fail, which then blinds the grid controller)
- Loss of Visibility: Cyber failures can render operators effectively “blind,” preventing informed and timely decision-making. This loss of situational awareness has been a primary contributing factor in several major historical blackout events.
- Complexity of Malicious Attacks: There is still a lack of comprehensive strategies to effectively address malware eradication and data recovery during cascading failure scenarios, where cyber and physical disruptions interact and amplify each other.



(A)Example CPPS model with interdependency.(B)Failure propagation in the power grid due to an initial failure in the power grid
(C)Power-dependent cyber network failure (D)Failure propagation in the cyber network due to its own failure
(E)Cyber-dependent power grid failure

Decentralization

- Mitigation Strategies: Using Distributed Energy Resources (DERs) and Edge Computing to reduce reliance on long-distance energy/data transfer.
- Self-Healing: Enabling local areas to achieve self-sufficiency, effectively "decoupling" interdependency during bulk grid failures

A Deep-Defense Approach for Next-Gen Cyber-Resilient Inter-Dependent Critical Infrastructure Systems

Eman Hammad

24 November 2021

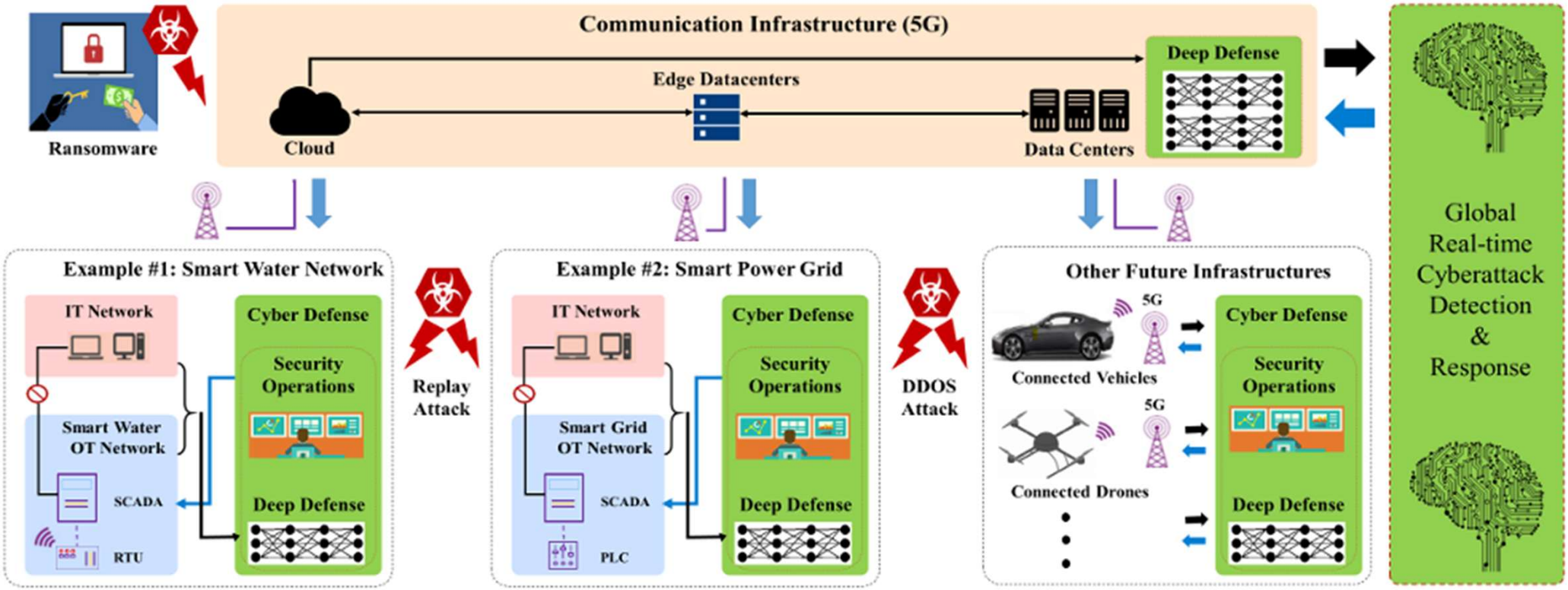
Next-Gen Critical Infrastructure (CI)

- Modern CI (electricity, water, transportation) is evolving to be more distributed, autonomous, and inter-connected to optimize resources
- Modeling infrastructures as Inter-dependent Cyber-Physical Systems (CPS) to systematically characterize threats across physical and cyber domains

Infrastructure Interdependency

- Increased inter-connectivity heightens the risk of failures in one system (e.g., the power grid) impacting others (e.g., water supply) in a potentially devastating cascading chain of events
- Blind spots exist due to a lack of visibility across multiple levels of individual and inter-connected CPS, leading to gaps in detection and recovery
- The smart grid plays a central role in enabling other CPS, meaning its stability is critical for the resilience of the entire ecosystem

Infrastructure Interdependency



Challenges to Cyber-Resilience

- Weak Situational Awareness: Current solutions often lack the visibility to detect complex "attack kill-chains" that exploit never-seen-before vulnerabilities.
- Integration Gaps: There is a weak coordination of adaptive-capacity resources (e.g., energy storage, reconfigurable networks) across cyber and physical layers.
- Legacy Issues: The mix of old and new technologies—many not designed with security controls—complicates the protection of inter-dependent networks.

The Deep-Defense Framework Architecture

- Data-Driven Defense: Utilizing telemetry and events from both Information Technology (IT) and Operational Technology (OT) domains to enrich situational awareness.
- Hierarchical Detection:
  - Local Module: Performs anomaly detection at the individual system level (e.g., smart water network).
  - Global Module: Uses 5G and edge technologies to correlate features from subsystems, detecting cross-correlated attacks and preventing cascading effects.
- Active Mitigation: Orchestrating available resources to identify, characterize, and recover from attacks in real time.

Advanced AI Technologies for Resilience

- Federated Learning (FL): Enables multiple actors to train robust detection models collaboratively without exchanging raw, sensitive data, thus preserving privacy and security.
- Generative Adversarial Networks (GANs): Used to synthesize cascading attack data for training, addressing the scarcity of real-world data on sophisticated inter-dependent infrastructure threats.
- Anomaly Detection: Leveraging Deep Learning (DL) to capture complex patterns and semantic knowledge of networks to flag global abnormalities