ACWAverse: An Interactive Cyber-Physical Water System Simulator for Security and Attack Analysis

1st Mehmet Oguz Yardimci
Department of Computer Science
Virginia Tech
Arlington, VA USA
oguzy@vt.edu

2nd Feras A. Batarseh
Department of Biological Systems Engineering
Virginia Tech
Arlington, VA USA
batarseh@vt.edu

Abstract—This paper presents ACWAverse, a comprehensive cyber-physical water system simulator designed for cybersecurity research, attack analysis, and intelligent system development. Utilizing its hydraulic simulation engine module, ACWAverse integrates advanced hydraulic modeling, water quality simulation, and sophisticated cyber-attack scenarios to create a powerful platform for cyber-physical security analysis. The system introduces novel capabilities including integrated cyber-attack simulation with duration-based effects, real-time data poisoning that affects both conditional actions and system visualization, and comprehensive attack modeling covering data poisoning, chemical interference, and physical damage scenarios. Key contributions include a modular, 4-layer architecture supporting unlimited network complexities, advanced attack simulation frameworks for vulnerability assessment, and extensive dataset generation capabilities for training machine learning models on cyber-physical contexts. The platform serves as a digital twin environment for water infrastructure, enabling meta-learning approaches for attack detection and response strategies. Performance evaluations demonstrate efficient simulation capabilities with comprehensive data export functionality for research applications. ACWAverse addresses critical gaps in cyber-physical security research by providing a powerful tool for developing, testing, and validating intelligent water management solutions, cyber-resilience strategies, and machine learning models for critical infrastructure protection.

Index Terms—Cyber-physical systems, attacks simulation, digital twin, dataset generation, water systems security.

I. Introduction

Water Supply Systems (WSS) are cornerstones of modern society, yet they face unprecedented challenges in the 21st century, including escalating demand, aging infrastructure, and sophisticated cyber threats [1]. Addressing these requires intelligent water systems with advanced sensing, AI, and robust control, necessitating sophisticated modeling tools. High-profile incidents such as the 2021 Oldsmar, Florida water treatment cyberattack [2], in which an intruder attempted to adjust chemical dosing to dangerous levels via remote access, underscore the real-world risks of data poisoning and unauthorized control in water utilities [3], [4].

Beyond Oldsmar, similar incidents continue to surface, including the 2024 Muleshoe, Texas water system compromise, where attackers manipulated controls, causing a municipal water tank to overflow before operators shifted to manual operations [5]. Such events in Muleshoe and nearby towns reinforce that cyber-physical risks are neither hypothetical nor isolated, and they directly motivate research platforms like ACWAverse that can replicate data-poisoning and unauthorized-control scenarios to evaluate detection and response strategies.

This work leverages the facilities of the ACWA Laboratory at Virginia Tech, including its instrumented physical testbed, PLC infrastructure, and curated datasets, which informed ACWAverse's requirements and provided ground truth for validation [6]. The original ACWA project [6] established a physical testbed for AI and cybersecurity experimentation, accompanied by a basic 2-tank digital twin simulator [7]. This simulator, while useful for validating physical results, was limited in scalability, modeling depth, and cyber scenario representation.

This paper introduces ACWAverse, a next-generation cyber-physical security research platform overcoming these limitations. It is a comprehensive simulation environment that concurrently models physical water distribution (hydraulics, quality) and sophisticated cyber-attack scenarios, creating a powerful tool for cybersecurity research and intelligent system development. This holistic approach is vital for understanding system behavior under normal and adversarial conditions, enabling the development of robust defense mechanisms. Key contributions include scalable network modeling far beyond the original 2-tank limit, advanced cyber-attack simulation frameworks with duration-based effects and real-time data poisoning, comprehensive dataset generation capabilities for training machine learning models in cyber-physical security, digital twin functionality for water infrastructure, and meta-learning approaches for attack detection and response strategies. ACWAverse serves as a research platform for investigating intelligent algorithms, assessing vulnerabilities, developing cyber countermeasures, and training machine learning models for critical infrastructure protection.

II. Related Work

Effective simulation tools are crucial for advancing research in intelligent water systems and their security. This

section reviews the original ACWA system's simulation component and compares ACWAverse with other tools.

A. Original ACWA System's Simulator Analysis

The original ACWA testbed's simulator [6] was a "software-based water digital twin" for its 2-tank system, primarily for validating physical experiments. Its limitations included significant scalability constraints due to the 2-tank design, preventing modeling of realistic networks. The simulation capabilities were basic, lacking advanced flow dynamics, comprehensive water quality kinetics for larger systems, and the means to simulate operational changes or cyber-attacks. Visualization was confined to basic dashboards, and its utility as a general research tool was hampered by its tight coupling to the specific physical setup. Critically, it was not designed to model cyber-attack scenarios. ACWAverse is engineered to address these specific shortcomings through a modern web-based approach.

B. Comparative Analysis with Existing Testbeds and Simulators

Physical testbeds like WaterBox [8], SWaT [9], and WADI [10] offer invaluable hands-on environments but can be costly, inflexible, and they create limited number of scenarios. Software simulators like EPANET [11] are industry benchmarks for hydraulic and water quality modeling. ACWAverse, while using similar hydraulic principles, differentiates itself through its integrated cyber-attack simulation capabilities, comprehensive dataset generation for machine learning, and digital twin functionality. It offers advanced cyber-physical security research capabilities, enabling the development and testing of machine learning models for attack detection and response. Furthermore, its modular architecture is tailored for integrating and testing custom AI algorithms and control strategies, positioning it as a strong platform for cybersecurity research and machine learning model development. Table I provides a comparative overview, highlighting ACWAverse's focus on cyber-physical security research, machine learning applications, and digital twin capabilities.

III. System Architecture

ACWAverse employs a modular, modern web-based architecture for scalability, extensibility, and universal accessibility, consisting of (1) Front-End Interface, (2) Simulation Engine, (3) Visualization Engine, and (4) Data Management layers. This 4-layered structure supports simulating both physical water system dynamics and cyber interactions, including sophisticated attack vectors, all within a browser environment.

A. Core Architecture Components

The system comprises four core architectural components designed for web-based operation. The front-end interface layer provides a modern and responsive web interface built with HTML5, CSS3 and JavaScript, featuring real-time network visualization, interactive component management, and dynamic form controls for simulation configuration.

The simulation engine is central, featuring three integrated modules running entirely in the browser. The hydraulic simulation module performs advanced fluid dynamics calculations (pipe flow, pump curves, valve logic, pressure distribution) using graph-based topology management. The water quality module offers comprehensive modeling of pH, DO, BOD, nitrate transport, disinfectant decay, and temperature with reaction kinetics. Crucially, the cyber-attack simulation module allows users to define and execute various cyber-attack scenarios, including data poisoning with duration-based effects, chemical interference, and physical damage, interfacing with the other modules to manipulate simulated sensor readings, alter actuator setpoints, or disrupt control logic.

The visualization engine introduces a sophisticated web-based approach, including Chart.js [12] for interactive time-series plots, custom HTML5 Canvas for network visualization, and multiple layout algorithms (topological sorting, balanced positioning, compact layout) for optimal network representation. The visualization includes real-time attack duration indicators and poisoned value display in graphs.

Finally, the data management layer handles JSON-based network configuration, simulation scenario definitions (including cyber-attack parameters), operational data, and results storage, with CSV export capabilities for further analysis.

B. Network Modeling Framework

ACWAverse uses a sophisticated framework representing water networks as directed graphs with detailed component properties. Nodes include sources (with flow specifications), tanks (with geometric properties, initial levels, and operational ranges), pumps (with efficiency modeling and power control), valves (with status control and characteristic settings), junctions (for flow distribution), and sinks (for demand representation). Edges represent pipes with diameter, length, roughness, and material properties. This detailed modeling enables accurate simulation of flow, pressure, and water quality in complex networks.

IV. Key Innovations

ACWAverse introduces significant innovations for water systems simulation, especially for intelligent systems and cyber security research in a web-based environment.

A core innovation is the integrated cyber-attack simulation framework with duration-based effects. This dedicated module allows users to model sophisticated attack vectors including data poisoning (with virtual sensor readings that affect both conditional actions and graph visualization), chemical interference (modifying water quality parameters), and physical damage (pump failures, valve

TABLE I
Comparison of Water System Testbeds and Simulators

Feature	Original ACWA [6]	EPANET/Others [11]	ACWAverse
Network Scale	2-tank limit	Scalable	Highly Scalable
Simulation Type	Basic hydraulic	Advanced Hydraulic + WQ	Advanced Hydraulic + WQ
Cyber-Attack Sim.	No	Limited/External	Integrated
User Interface	Desktop-based	Desktop-based	Web Interface
Visualization	Basic Dashboards	Basic/Static	Real-time, Interactive Web
Accessibility	Local only	Local installation	Web-based, Cross-platform
Real-time Aspects	Physical only	Offline Simulation	Real-time Web Simulation
Hybrid C-P Focus	Digital Twin	Primarily Physical	Cyber + Physical Sim.
Ease of Use	Easy	Difficult	Easy

malfunctions, leaks). Attacks can be scheduled with specific durations and timing, and their effects are visualized in real-time with duration indicators on graphs.

The platform provides advanced layout algorithms for network visualization. This includes topological sorting for layouts based on logical flow, balanced positioning for optimal space utilization, and compact layouts for dense network representation. These algorithms automatically adjust component positioning based on network complexity and user preferences.

Real-time data poisoning with visual feedback capabilities represents a quantum leap in cyber-attack simulation. The system can inject false sensor readings for specified durations, affecting both conditional action evaluation and graph visualization, providing immediate visual feedback on attack impacts.

In addition, comprehensive sample systems and educational features are prioritized. Pre-configured systems range from simple loops to complex real-world topologies like the Muleshoe Water System, enabling immediate experimentation and learning. The web-based interface enables remote access and collaboration without installation barriers.

Lastly, the web-based accessibility and real-time visualization, eliminating the need for desktop installation. The platform runs entirely in modern browsers, providing cross-platform compatibility, real-time network visualization with multiple layout algorithms, and interactive data exploration without software installation requirements.

V. Implementation Details

ACWAverse leverages modern web technologies and robust numerical methods for browser-based simulation.

A. Web-based architecture implementation

The ACWAverse system is built using HTML5, CSS3, and vanilla JavaScript, ensuring broad browser compatibility without external dependencies. The front-end uses Tailwind CSS for responsive design and Chart.js for interactive data visualization. The simulation engine runs entirely client-side, providing real-time performance without server requirements.

B. Hydraulic simulation engine

The ACWAverse engine is advanced by solving the network continuity and energy relations iteratively. Pipe headloss is represented either by the Hazen–Williams form,

$$h_{f,i} = K_i \, Q_i^{n}, \tag{1}$$

or by the Darcy–Weisbach form,

$$h_{f,i} = f_i \, \frac{8 \, L_i}{\pi^2 g D_i^{5}} \, Q_i^{2}, \tag{2}$$

where the friction factor f_i may depend on flow Q_i and roughness ε [13]–[15]. Pump head is modeled by a characteristic curve,

$$H_p(Q) = a_0 + a_1 Q + a_2 Q^2, \tag{3}$$

while valve losses are captured by

$$h_v = K_v(\sigma) \, \frac{Q^2}{2gA^2}, \tag{4}$$

with σ denoting the valve opening. Mass continuity at junctions is enforced as

$$\sum_{\text{in}} Q \; - \; \sum_{\text{out}} Q = 0, \tag{5}$$

and tank water level Y_t is updated by

$$\frac{\mathrm{d}Y_t}{\mathrm{d}t} = \frac{Q_{\text{in}}(t) - Q_{\text{out}}(t)}{A_t(Y_t)}, \tag{6}$$

where $A_t(Y_t)$ denotes the cross-sectional area at level Y_t. The network energy balance is imposed via

$$\sum \left(\frac{p}{\gamma} + z + \frac{V^2}{2g} \right) - h_L = \text{const.} \tag{7}$$

The nonlinear system composed of Equation [5]-Equation [7] is solved at each step prior to updating the quality states.

C. Water quality modeling

Transport and transformation of constituents are simulated in coupled fashion. Dissolved oxygen obeys

$$\frac{\mathrm{d}C_{O_2}}{\mathrm{d}t} = P_{\mathrm{reaer}}(C_{O_2}, T) - k_{O_2} C_{O_2} + \text{mixing}, \tag{8}$$

biochemical oxygen demand follows

$$\frac{\mathrm{d}C_{\mathrm{BOD}}}{\mathrm{d}t} = -k_{\mathrm{BOD}}\, C_{\mathrm{BOD}} + \text{mixing}, \tag{9}$$

and inorganic carbon/CO_2 balance is written as

$$\frac{\mathrm{d}C_{\mathrm{CO_2}}}{\mathrm{d}t} = S_{\mathrm{CO_2}} - k_{\mathrm{str}} C_{\mathrm{CO_2}} + \text{mixing}. \tag{10}$$

The resulting pH is given by

$$\mathrm{pH} = -\log_{10}\left[H^+\right], \text{with charge balance } f\left([H^+], \mathrm{ALK}, C_{\mathrm{CO_2}}\right) = 0. \tag{11}$$

Water temperature is updated by the energy balance

$$\frac{\mathrm{d}T}{\mathrm{d}t} = \frac{UA}{mc_p}\left(T_{\mathrm{air}} - T\right) + \text{advection}, \tag{12}$$

and nitrate dynamics are represented by

$$\frac{\mathrm{d}C_{\mathrm{NO_3}}}{\mathrm{d}t} = -k_{\mathrm{NO_3}}\, C_{\mathrm{NO_3}} + \text{mixing}. \tag{13}$$

Inter-unit exchange is modeled as a perfectly mixed transfer,

$$\frac{\mathrm{d}C_T}{\mathrm{d}t} = \frac{1}{\mathrm{Vol}_T}\left(\sum_i Q_{\mathrm{in},i} C_{\mathrm{in},i} - \sum_j Q_{\mathrm{out},j} C_T\right) + R(C_T). \tag{14}$$

D. Cyber-attack simulation implementation

Four cyber-physical perturbation modes are supported and are referenced at the start of the section: chemical dosing for pH control *Equation* [20], chemical interference on quality states *Equation* [16], physical damage that alters hydraulic or storage parameters *Equation* [17], and data poisoning of sensor streams *Equation* [15]. These mechanisms are scheduled by the scenario engine and are evaluated at each integration step concurrently with the plant model.

a) Data poisoning.: Virtual sensor readings are modified over a programmed window,

$$P'_{\mathrm{sensor}}(t) = P_{\mathrm{actual}}(t) + \Delta P_{\mathrm{attack}}, \qquad t \in [t_{\mathrm{start}}, t_{\mathrm{end}}], \tag{15}$$

so that both conditional logic and visualization ingest the altered values.

b) Chemical interference.: State variables are directly offset,

$$C_{\mathrm{new}} = C_{\mathrm{orig}} + \Delta C_{\mathrm{attack}}, \tag{16}$$

which emulates contamination or reagent misdosing.

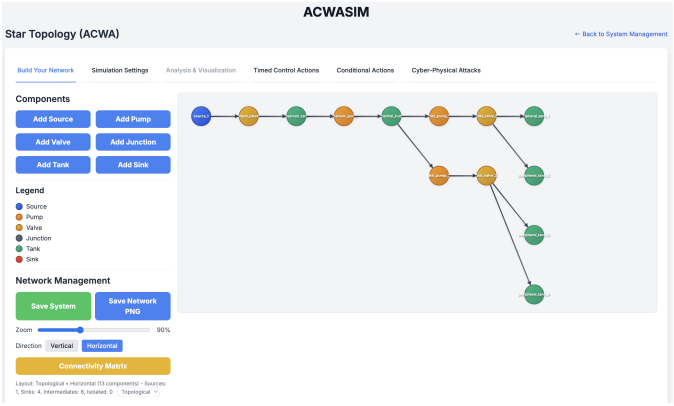

Fig. 1. ACWAverse web interface showing network builder and analysis tabs.

c) Physical damage.: Component states are forced to degraded modes, for example pump failure,

$$P_{\mathrm{pump}} = 0, \tag{17}$$

valve freeze,

$$V_{\mathrm{status}}(t) = V_{\mathrm{status}}(t_0), \tag{18}$$

and leak introduction,

$$Q_{\mathrm{leak}} = \alpha\, Q_{\mathrm{orig}}, \quad 0 < \alpha < 1. \tag{19}$$

d) Acid dosing for pH control.: An instantaneous dose is represented by

$$C_{H^+}^{\mathrm{new}} = C_{H^+} + \Delta C_{\mathrm{dose}}, \tag{20}$$

with the updated pH computed via Equation [11]. Real-world incidents are noted to underscore the operational risk of such manipulations [3], [4].

E. Visualization implementation

The ACWAverse web interface uses HTML5 Canvas for network visualization with custom rendering algorithms. Chart.js provides interactive time-series plots with attack duration annotations. Multiple layout algorithms are implemented. An overview of the interface is shown in Fig. 1.

Topological layout: Uses Kahn's algorithm for topological sorting with BFS-based level assignment [16].

Balanced layout: Grid-based positioning with type-based grouping and collision avoidance.

Compact layout: Dense positioning for space-efficient visualization.

VI. System UI

Figure 2 shows the updated entry screen where users can either load a bundled sample, import a saved JSON system, or create a new system from scratch. For distribution-style testbeds, the tool ships with an ACWA-inspired topologies. These presets provides a quick starting point for scenario generation and controller benchmarking.

Component creation and layout controls are consolidated in a right-side panel (Fig. 3). From here the user can

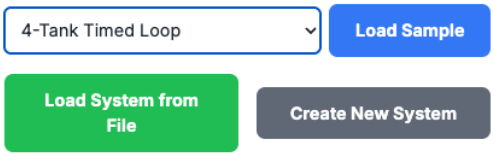

Fig. 2. Entry screen with sample selector, Load System from File, and Create New System.

add sources, pumps, valves, junctions, tanks, and sinks; adjust zoom and orientation; save the system; and export a PNG of the network schematic.

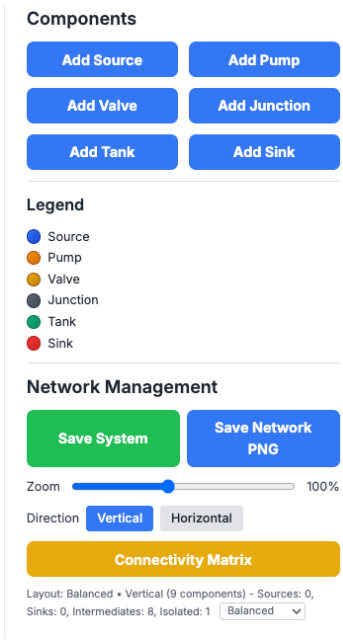

Fig. 3. Components and network management panel.

The connectivity between tanks, pumps, valves, and other elements is now edited via a matrix view (Fig. 4), where rows denote sources (from) and columns denote destinations (to). This makes directionality explicit and prevents ambiguous links.

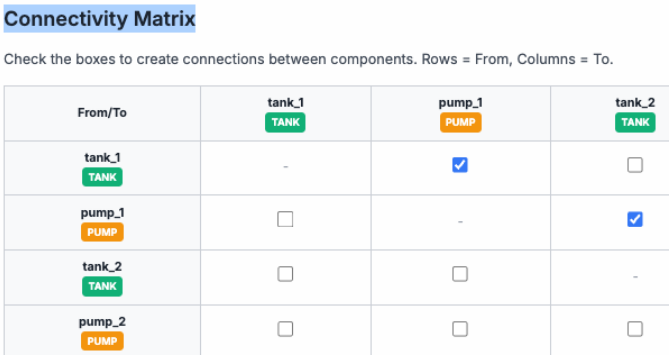

Fig. 4. Connectivity Matrix. Rows are from components and columns are to components; checked cells create directed edges.

Global parameters and initial states are defined prior to execution (Fig. 5). In our experiments we ran 900 s simulations at 20 °C ambient temperature with specified initial levels and water quality states per tank.

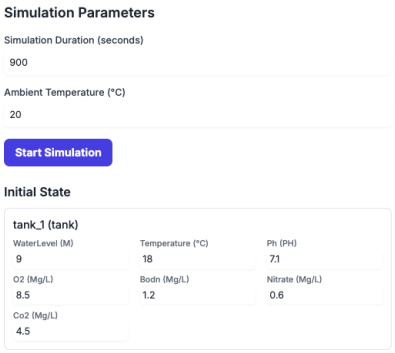

Fig. 5. Simulation parameters with initial state preview.

Users can program both time-driven controls (Fig. 6) and state-driven conditional logic (Fig. 7). Timed actions schedule changes at specific timestamps, whereas conditional rules react to sensor thresholds during the simulation. Together, these cover typical supervisory control use cases and cyber-physical test scenarios.

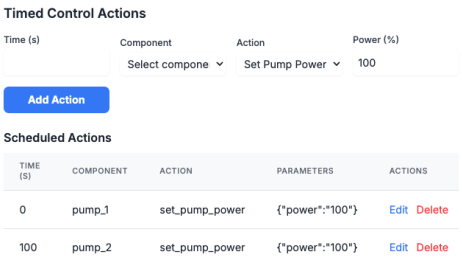

Fig. 6. Timed control actions GUI.

ACWAverse includes a library of cyber-physical attack scenarios (Fig. 8) for studies. These allow injecting pH dosing events, chemical interference, physical damage, or data poisoning on selected components at runtime, enabling repeatable stress tests for resilience analysis.

After a run, per-component diagnostics are available (Fig. 9), including water level, volumetric amount, power, and temperature traces. Results can be exported to CSV to reproduce the plots offline and to support statistical comparisons across trials.

VII. Research Applications and Use Cases

ACWAverse serves as an open access comprehensive research platform for cyber-physical security, machine learning, and digital twin applications in water infrastructure systems.

A. Cyber-Physical Security Research

ACWAverse provides a comprehensive environment for cyber-physical security research, enabling the study of

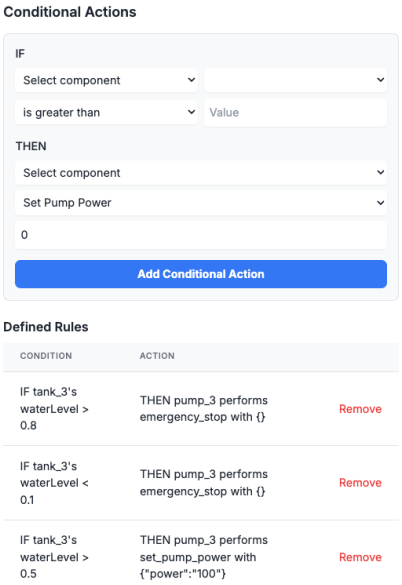

Fig. 7. Conditional (event-driven) actions GUI.

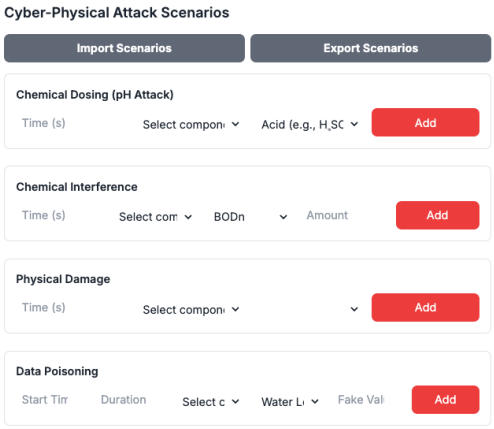

Fig. 8. Cyber-physical attack scenarios panel.

attack propagation, system resilience, and defense mechanism effectiveness. Researchers can investigate how cyber-attacks affect physical system behavior, study attack cascading effects, and develop countermeasures for critical infrastructure protection. The platform supports vulnerability assessment, threat modeling, and security protocol validation, providing insights into the complex interactions between cyber and physical systems.

B. Dataset Generation for Machine Learning

ACWAverse provides extensive capabilities for generating synthetic datasets for machine learning research in cyber-physical security. The platform can generate diverse attack scenarios with varying parameters, timing, and intensities, creating labeled datasets for training supervised learning models. The system supports batch simulation runs with different network configurations,

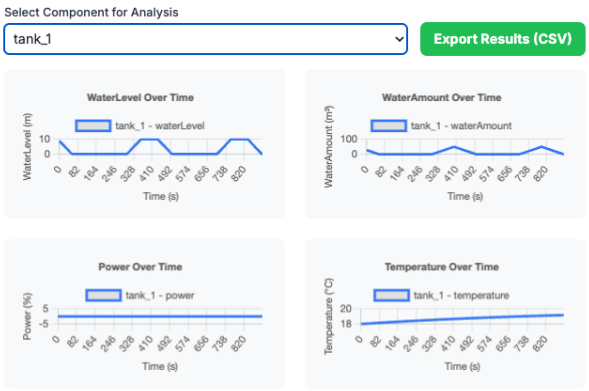

Fig. 9. Per-component time series plots and CSV export.

attack types, and environmental conditions, enabling the creation of large-scale datasets for deep learning applications. Generated datasets include time-series data with attack annotations, system state information, and performance metrics, providing comprehensive training data for anomaly detection, attack classification, and predictive modeling algorithms.

C. Digital Twin Functionality

ACWAverse serves as a digital twin environment for water infrastructure systems, enabling real-time monitoring, predictive maintenance, and cyber-resilience assessment. The platform can be configured to mirror real-world water systems, providing a virtual representation for testing control strategies and security measures before deployment. Digital twin capabilities include real-time state synchronization, predictive modeling of system behavior, and virtual testing of cyber-attack scenarios without risk to physical infrastructure. This functionality enables the development of robust defense mechanisms and the validation of security protocols in a safe, controlled environment.

D. Meta-Learning for Attack Detection

The platform supports meta-learning [17] approaches for developing adaptive attack detection and response strategies. By generating diverse attack scenarios and system configurations, ACWAverse enables the training of meta-learning models that can quickly adapt to new attack types and system variations. The system's ability to simulate different attack patterns, timing, and intensities allows researchers to develop models that generalize across various cyber-physical threats. Meta-learning applications include few-shot learning for new attack detection, adaptive anomaly detection, and transfer learning for different water system topologies.

VIII. Case Studies and Examples

ACWAverse offers a rich feature set for research in intelligent water systems and cyber security through its

web-based platform. For network design and management, it provides an intuitive web interface for visual network creation with drag-and-drop capabilities and an extensive component library. Users can leverage pre-configured sample systems, import/export data in JSON format, and manage multiple scenarios through the browser interface.

Simulation configuration and control is highly flexible through the web interface. Users can define simulation duration and time steps, easily modify physical parameters and operational settings, and utilize dedicated interfaces for defining cyber-attack scenarios (type, target, parameters, timing, duration). The system supports testing various control strategies, from simple rules to advanced conditional actions, and offers real-time simulation control.

Key parameters are monitored in real-time through interactive web dashboards. The system generates detailed time-series data for all components with export capabilities. It supports multi-parameter visualization, temporal trend analysis with statistics, and spatial distribution maps. Specific metrics and visualizations are available for attack impact assessment, including duration-based attack indicators and poisoned value visualization.

To illustrate ACWAverse's capabilities, several case studies are presented demonstrating the platform's versatility and practical applicability.

A. 4-Tank Conditional Loop

This topology demonstrates the integrated cyber-attack framework and conditional control logic. A 4-tank loop system with conditional actions based on tank levels is subjected to data poisoning attacks. The attack targets tank level sensors, injecting false readings for specified durations. Objectives include observing pump control responses to poisoned data, determining physical consequences, and evaluating the visual feedback system. The simulation demonstrates how poisoned sensor readings trigger false conditional actions, leading to system instability, with the effects clearly visualized in both the network display and time-series graphs with attack duration indicators.

B. ACWA Topologies Network

These topologies showcase ACWAverse's ability to handle complex network topologies and multiple attack scenarios. A star topology system with a central hub and peripheral distribution is subjected to various attack types including data poisoning, chemical interference, and physical damage. The system demonstrates how different layout algorithms (topological, balanced, compact) can be used to visualize the same network effectively. The case study shows how attacks propagate through the network and affect different components, with real-time visualization of attack impacts and duration-based effects.

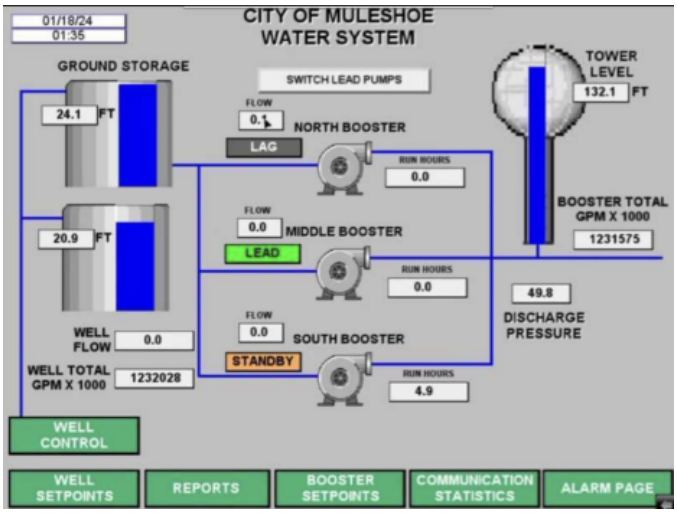

Fig. 10. Muleshoe Water System visualization used in ACWAverse case study (image context and incident details per [18]).

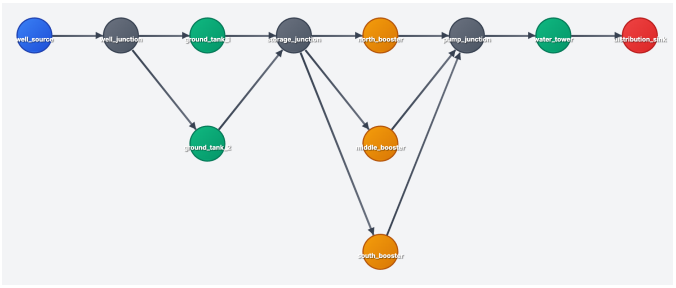

Fig. 11. ACWAverse replication of the Muleshoe network layout corresponding to Fig. 10. [18]

C. Muleshoe Water System: Real-World Topology

This topology demonstrates ACWAverse's capability to model real-world water distribution systems. The Muleshoe Water System, representing a typical municipal water distribution network, is implemented with proper junctions, booster pumps, and distribution patterns. The system includes realistic flow rates, tank capacities, and operational parameters. This case study shows how ACWAverse can be used for practical water system analysis, including vulnerability assessment and cyber-resilience testing on realistic infrastructure models. Fig. 10 illustrates a representative HMI view of the Muleshoe system, and Fig. 11 shows the corresponding ACWAverse replication used in our experiments.

D. Visualization and Layout Algorithms

A comprehensive comparison of ACWAverse's visualization capabilities demonstrates the effectiveness of different layout algorithms. The same network is visualized using topological, balanced, and compact layouts, showing how each algorithm optimizes different aspects of network representation. The comparison includes real-time attack visualization with duration indicators, poisoned value

display in graphs, and interactive data exploration capabilities. These case studies exemplify ACWAverse's utility in tackling diverse water system challenges through its web-based platform.

IX. Evaluation and Results

ACWAverse's performance, accuracy, and usability are evaluated in a web-based environment. Performance analysis revealed efficient browser-based simulation capabilities. For complex networks (50+ nodes, 70+ pipes), 24-hour simulations complete within seconds in modern browsers, demonstrating the effectiveness of client-side computation. Memory utilization scales reasonably, with a 100-component network using under 100MB of browser memory. Scalability tests on networks with over 500 components demonstrated practical performance for research applications in web environments.

Accuracy validation against established benchmarks showed strong results. Hydraulic calculations (flow, pressure) deviated less than 2% from theoretical expectations for identical configurations. Pump and valve operations matched theoretical behavior. Water quality modeling, including tracer transport and first-order decay, agreed well with analytical solutions (typically within 5% for concentrations). Simulated physical consequences of cyber-attacks are consistent with logical expectations, validating the cyber module's interface with physical models.

Usability evaluation demonstrated significant improvements in accessibility. The web-based interface eliminates installation barriers, enabling immediate access from any device with a modern browser. The intuitive interface allows users to create complex networks and configure sophisticated attack scenarios without specialized training. Real-time visualization with multiple layout options enhances understanding of system behavior and attack impacts.

X. Conclusion

ACWAverse is a foundation for continued development in web-based cyber-physical simulation. Future advanced modeling capabilities include tighter AI/ML integration for training models, using ML as soft sensors or AI adversaries; incorporating Uncertainty Quantification (UQ) techniques; multi-physics coupling with groundwater, structural, or power system models; modules for advanced water treatment processes; and integrating real-time optimization algorithms.

Enhanced cyber-security features will involve expanding the attack library (Man-in-the-Middle, protocol-specific attacks), enabling simulation of defense mechanisms (IDS, resilient controls), and modeling cyber-physical co-evolution of attacks and defenses.

Improved usability and collaboration may see cloud-based deployment options, collaborative design tools, version control integration, and strengthened digital twin capabilities with real-time data ingestion and model calibration.

Industry and educational integration efforts will focus on SCADA/PLC interfaces for Hardware/Software-in-the-Loop simulation, expanded support for industry standards, dedicated educational modules and tutorials, and features for regulatory reporting assistance.

ACWAverse represents a transformative advancement in cyber-physical security research, addressing critical gaps in cybersecurity research for water infrastructure systems and introducing revolutionary capabilities for machine learning, digital twin applications, and meta-learning approaches. Its comprehensive cyber-physical approach, integrating advanced hydraulic/water quality modeling with sophisticated cyber-attack simulation frameworks, enables a holistic understanding of system behavior under normal and adversarial conditions, providing a powerful platform for developing intelligent defense mechanisms.

Key achievements include scalable network modeling beyond the 2-tank limit, advanced cyber-attack simulation with duration-based effects and real-time data poisoning, comprehensive dataset generation capabilities for machine learning research, digital twin functionality for water infrastructure, and meta-learning approaches for adaptive attack detection. The integrated cyber-attack simulation module, particularly the data poisoning capabilities that affect both conditional actions and system visualization, is invaluable for training machine learning models and developing cyber-resilience strategies.

Evaluations confirm efficient simulation capabilities, validated accuracy, and comprehensive data export functionality for research applications. The modular architecture ensures adaptability for future research needs in cyber-physical security. ACWAverse significantly contributes to addressing global cybersecurity challenges in critical infrastructure by providing a powerful research platform for developing, testing, and validating machine learning models, digital twin applications, and intelligent defense mechanisms. Its continued development will foster innovation in cyber-physical security research and help develop the next generation of intelligent, resilient, and secure water systems.

References

[1] F. A. Batarseh, J. Chandrasekaran, and L. J. Freeman, "An introduction to ai assurance," in AI Assurance. Elsevier, 2023, pp. 3–12.

[2] N. LaLone, "Chapter 13 - on the growing importance of routine cybersecurity: The oldsmar water plant "hack"," in Case Studies in Disaster Response, ser. Disaster and Emergency Management: Case Studies in Adaptation and Innovation, S. Feldmann-Jensen, S. J. Jensen, and J. Slick, Eds. Butterworth-Heinemann, 2024, pp. 237–248. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128095263000117

[3] J. Cervini, A. D. Rubin, and L. A. Watkins, "Don't drink the cyber: Extrapolating the possibilities of oldsmar's water treatment cyberattack," in International Conference on Cyber Warfare and Security, 2022.

[4] CISA, FBI, and EPA, "Compromise of u.s. water treatment facility," Joint Cybersecurity Advisory AA21-042A, February 2021, accessed: 2025-09-11. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

[5] A. Press, "Cyberattack causes muleshoe, texas water tank overflow; sandworm implicated," AP News, 2024, accessed: 2025-09-11. [Online]. Available: https://apnews.com/article/5f388bf0d581fc8eb94b1190a7f29c3a

[6] F. A. Batarseh, A. Kulkarni, C. Sreng, J. Lin, and S. Maksud, "Acwa: An ai-driven cyber-physical testbed for intelligent water systems," Water Practice & Technology, vol. 18, no. 12, pp. 3399–3418, 2023.

[7] F. Batarseh, A. Kulkarni, C. Sreng, L. J., and S. Maksud, "Acwa data," 2023. [Online]. Available: https://github.com/AI-VTRC/ACWA-Data

[8] S. Kartakis, E. Abraham, and J. A. McCann, "Waterbox: A testbed for monitoring and controlling smart water networks," in Proceedings of the 1st ACM International Workshop on Cyber-Physical Systems for Smart Water Networks, 2015, pp. 1–6.

[9] A. P. Mathur and N. O. Tippenhauer, "SWaT: a water treatment testbed for research and training on ICS security," in 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), 2016.

[10] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "Wadi: a water distribution testbed for research in the design of secure cyber physical systems," in Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, 2017, pp. 25–28.

[11] L. A. Rossman, "Epanet 2: Users manual," U.S. Environmental Protection Agency, Cincinnati, OH, Tech. Rep. EPA/600/R-00/057, 2000.

[12] Chart.js Developers, "Chart.js: Simple, clean and engaging charts for designers and developers," https://www.chartjs.org/, 2025.

[13] C. F. Colebrook, "Turbulent flow in pipes, with particular reference to the transition region between the smooth and rough pipe laws," Journal of the Institution of Civil Engineers, vol. 11, no. 4, pp. 133–156, 1939.

[14] L. F. Moody, "Friction factors for pipe flow," Transactions of the ASME, vol. 66, pp. 671–684, 1944.

[15] P. K. Swamee and A. K. Jain, "Explicit equations for pipe-flow problems," Journal of the Hydraulics Division, vol. 102, no. 5, pp. 657–664, 1976.

[16] A. B. Kahn, "Topological sorting of large networks," Communications of the ACM, vol. 5, no. 11, pp. 558–562, 1962.

[17] J. Schmidhuber, "Evolutionary principles in self-referential learning. on learning now to learn: The meta-meta-meta...-hook," Diploma Thesis, Technische Universitat Munchen, Germany, 14 May 1987. [Online]. Available: http://www.idsia.ch/ juergen/diploma.html

[18] M. Kan, "Russia may be behind hack of texas water facility," PCMag, April 2024, accessed: 2025-09-11. [Online]. Available: https://www.pcmag.com/news/russia-may-be-behind-hack-of-texas-water-facility