IoT Security and Safety Testing Toolkits for Water Distribution Systems

Sean O'Toole, Cameron Sewell, Hoda Mehrpouyan
Department of Computer Science
Boise State University
Boise, United States
seanotoole@u.boisestate.edu, cameronsewell@u.boisestate.edu, hodamehrpouyan@boisestate.edu

***Abstract*—Due to the critical importance of Industrial Control Systems (ICS) to the operations of cities and countries, research into the security of critical infrastructure has become increasingly relevant and necessary. As a component of both the research and application sides of smart city development, accurate and precise modeling, simulation, and verification are key parts of a robust design and development tools that provide critical assistance in the prevention, detection, and recovery from abnormal behavior in the sensors, controllers, and actuators which make up a modern ICS system. However, while these tools have potential, there is currently a need for helper-tools to assist with their setup and configuration, if they are to be utilized widely. Existing state-of-the-art tools are often technically complex and difficult to customize for any given IoT/ICS processes. This is a serious barrier to entry for most technicians, engineers, researchers, and smart city planners, while slowing down the critical aspects of safety and security verification. To remedy this issue, we take a case study of existing simulation toolkits within the field of water management and expand on existing tools and algorithms with simplistic automated retrieval functionality using a much more in-depth and usable customization interface to accelerate simulation scenario design and implementation, allowing for customization of the cyber-physical network infrastructure and cyber attack scenarios. We additionally provide a novel in-tool-assessment of network's resilience according to graph theory path diversity. Further, we lay out a roadmap for future development and application of the proposed tool, including expansions on resiliency and potential vulnerability model checking, and discuss applications of our work to other fields relevant to the design and operation of smart cities.**

***Index Terms*—smart cities, internet of things, operational technology, industrial control systems, critical infrastructure, simulation, toolkits, software development, safety, resilience**

I. Introduction

As a result of general increases in malicious cyber activity in recent years, and in the wake of STUXNET, the cyber security of industrial control systems is increasingly becoming a massive security concern for cities, companies, and nations [1], [2]. The most prominent types of attacks have usually targeted the Information Technology (IT) components of a system. These attacks are usually conducted for financial gain and usually do not cause long term damage to the systems being affected, especially if there is a significant separation between data management and the actual operational technology (OT). For example, the recent Colonial Pipeline attacks, which were IT-based and targeted billing information. Colonial themselves shut down their own pipeline until the ransomware issue was resolved and there was no structural damage done to the pipeline [3]. If, however, they were targeted with an OT-focused attack that took control of operational devices, sensors, or actuators within the ICS, the attackers could have created serious physical damage in the over 5,500-mile-long pipeline that could have caused millions of dollars damage and left up to 45 percent of the East Coast of the United States without gas for an undetermined amount of time.

An example of the full potential damage of an OT attack could be seen in the 2007 INL Aurora Generator test [4], which created abnormal vibrations in a diesel generator within 13 iterations of the attack loop and eventually caused the engine to dramatically fail. Manipulation of the control logic which controlled the generator led to significant physical damage, a methodology that would be similarly applied in the cyber worm STUXNET several years later in an attack against the country of Iran's nuclear refinement capabilities to significant effect.

In the years since, an increasing number of attacks have sought to utilize tools like this against city and regional infrastructure. In 2015, several regions of Ukraine's energy grid were affected by an attack, leaving 225,000 people without power. And again in 2016 a power grid hack affecting a key substation shut down one fifth of power traffic in the city of Kyiv. Following the 2016 attack the President of Ukraine, Petro Poroshenko, stated that state institutions had been targeted about 6,500 times in the final months of that year [5]. 2017's TRITON attacks against Saudi Arabian natural gas processing plants represented a near-miss, where the potential for serious physical damage and threat to human life was only avoided by a single fail-safe missed by attackers [6]. In regards to water distribution systems, the Oldsmar Water Plant Attack in Feb. 2021 is the most recent example [7], following on the heels of the April 2020 attacks against multiple regional water systems in Israel [8], both of which sought to dump toxic levels of chlorine into the water, presenting a serious threat to the health and well being of citizens. However, OT threats to water go back further, all the way to the 2000 Maroochy water plant incident, in which hundred of thousands of gallons of untreated sewage were dumped back into local water supplies by a single attacker with access to OT systems

Funding provided under a grant from the National Science Foundation.

[9]. For a more thorough review of cyber attacks against ICS in general, we refer the reader to an excellent review of incidents up to 2018 in Hemsley et al. [10]. To better protect our critical infrastructure we need to understand exactly how these OT attacks affect our infrastructure so that we can create safe guards to protect against them. We additionally need to develop ways to better prepare and train the professionals in the field for incidents such as these. For this, accessible and usable tools are badly needed.

The rest of the paper is organized as follows: Section 2 provides context for the application of simulation in various fields for the purpose of improving safety and security in systems and procedures, as well as more specifically those targeting the needs of smart cities. Section 3 describes state-of-the-art simulation toolboxes for Water Distribution Systems (WDS) which could be used for research and practical testing of hydraulic systems models. Section 4 introduces *inp2cpa* [11] and the changes we have made to the tool in order to make file conversion and creation more accessible and streamlined, as well as our contribution of network graph theory resiliency model checking, and briefly discusses future plans for the work, which is expanded upon in Section 5. Finally, Section 5 summarizes the work, and more thoroughly outlines future plans and goals for *inp2cpa* moving forwards.

II. Simulation for Improving Safety and Security

Simulation here refers to the replication of real-world processes with cyber and cyber-physical tools and programs by means of mathematical equations and programmatic structures which capture, as closely as possible, the key characteristics of the system being simulated. We will address some of the many ways in which simulation has been used to improve safety and security outcomes, and then focus in on open-source toolkits for smart city IoT simulation applications in order to identify those which would be useful for cities to test and improve on their systems without needing to rely on or expend heavily into proprietary software.

Many fields have incorporated simulation into their education and training to yield well-educated individuals at lower cost and less danger to the individual in-the-field training. The precursor to modern simulation training was first tested in 1978 by the National Aeronautics and Space Administration, who found in their studies of disasters that most aviation accidents involved a lack of leadership coordination, or decision making [12]. Simulations also spread to the maritime world focusing on on the same issues. Most high fidelity maritime simulations reproduce the pilot or captains room and the engine room to inundate the crew with the auditory and visual factors they will need to expect while on the job [13]–[15]. The formalization of simulation-based educational practices has advanced in the medical industry as well due to the development of international and national multidisciplinary societies, usually aimed at a broad membership of healthcare educators, clinicians, researchers and engineers, and supported by industry [16]. These simulation training sessions better prepare individuals for the needs of different scenarios than standard training, reducing accidents and waste. In all cases, simulation could be applied to improve safety outcomes for both those doing the work and those relying on their efforts.

Within those subset of simulators targeting the needs of smart cities and considering the role of IoT devices within those cities, and which are seeing ongoing development and maintenance, several exist which allow for relatively thorough simulation of various network, power, and IoT simulation. Simulation of Urban Mobility (SUMO) is one of the oldest and best examples of the kind of toolset that can be of great benefit to a city, offering a powerful tool for analyzing road networks and traffic patterns and experimenting on them, before returning to users simulated traffic data, physical effect data, and improved road networks if desired by the user [17].

Bonceur's CupCarbon [18] is perhaps the best example of a modern smart city simulation tool with the capability of modeling real-world scenarios and their impacts on and interactions with a specific subset of city infrastructure. Bounceur proposed and later presented CupCarbon in 2017 as a flexible simulation tool focused on radio propagation channels and IoT interactions within a user-designated network and set against real-world maps. CupCarbon allows for the simulation of wireless network behavior and communication with a large number of different components and customizable parameters, and most notably allows for designing scenarios in which real-world events such as fire incidents and gas leaks can be simulated, with the event having an effect on the ability of the network to communicate clearly. Custom python scripts can be written for different nodes, allowing for potentially limitless variety and customization of system behavior. However, with few examples and no capability of importing existing files on which to base designs, the tool is currently inhibited by its lack of user accessibility and the lack of training available for it.

It is our goal with this work to help streamline the process of simulation in industrial control system security and infrastructure resilience, as well as bring better physical systems simulation and OT more into focus when discussing smart city infrastructure and security.

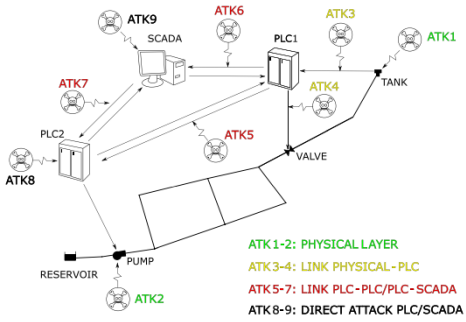

Fig. 1. epanetCPA Attack Modeling Approach - "Characterizing Cyber-Physical Attacks on Water Distribution Systems," Toarmina et al. [19]

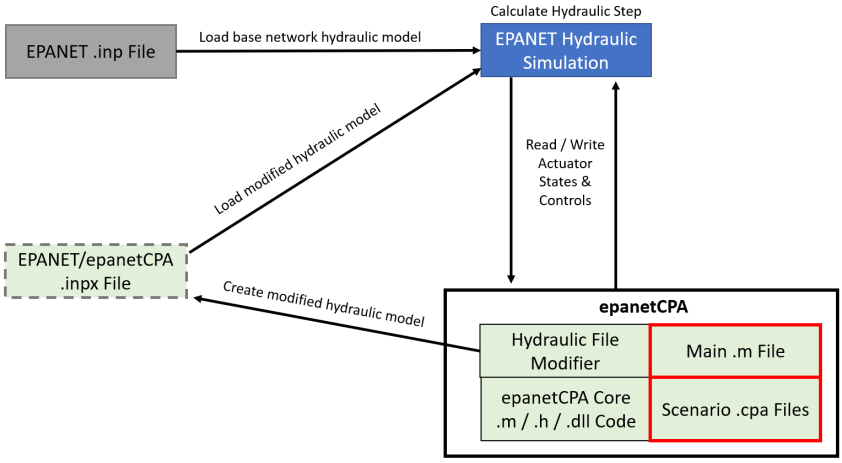

Fig. 2. File requirements for epanetCPA configuration. Red indicates user creation required.

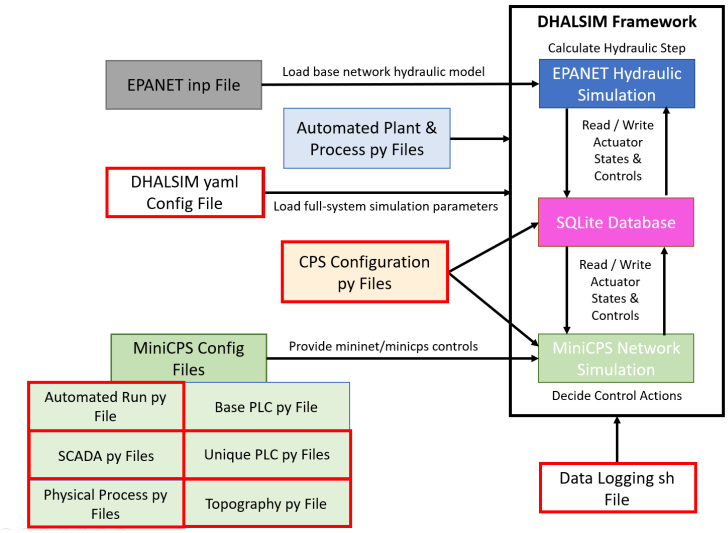

Fig. 3. File requirements for DHALSIM configuration. Red indicates user creation required.

III. State-of-the-Art Safety and Security Testing Toolboxes in WDS

A variety of open-source tools have been created to address the threat of OT attacks, specifically in water distribution. Among these, the two we find to be most significant in terms of contribution and potential for future development in recent years are Taormina et al.'s epanetCPA [19] and Murillo et al's. DHALSIM [20]. Taormina et al. and his team created epanetCPA, a MATLAB based program for modeling the response of water systems to cyber-physical attacks that runs on top of EPANET. EPANET is used world wide by engineers and researches to design new water infrastructure, update existing water systems, and develop more efficient solutions to solve water quality problems. It is a Windows based software application for simulating and representing water distribution systems. It uses a network configuration or .inp file which represents a physical water system and creates a digital representation of the water network, representing all pipes, junctions, tanks, reservoirs, valves, and pumps. epanetCPA works in tandem with EPANET modifying the input file with information from a user provided cyber-physical attack file, .cpa. The changes in file information create a new data set seperate from the ground truth and diplayed by the EPANET model analysis. Murillo et al. in "Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments" introduced Digital Hydraulic Simulator (DHALSIM) [21] to show the physical processes, control logic, and network communication of a cyber-physical system while it is under attack. DHALSIM provides users a full network capture of the PLCs, SCADA systems, and any other network device present on the system.

However, although both toolkits offer considerable utility, creating custom scenarios and models for each requires considerable work on the part of the user, and the prerequisite knowledge of the programming languages and/or file formats in use within each toolkit. As can be seen in Fig. 2 and

Fig. 3, multiple files of different formats and languages are required for each of epanetCPA and DHALSIM, although the added complexity of DHALSIM in attempting to co-simulate network behavior results in requiring significantly many more custom files and configurations. This is a non-trivial issue for research and application of these toolkits going forward, if they are to be utilized for safety and security testing and training. While some understanding of programming is not an unreasonable expectation for users, the current toolkits require an in-depth understanding of the toolkits themselves, along with the formats and langauges in use, in order to customize to any significant degree. Cutting down on this requirement would make them vastly more approachable and usable. We believe that *inp2cpa* and expansion of its current functionality, and the creation of tools like it for other simulation toolkits in WDS and general ICS simulation, is a critical part of lowering that barrier to entry.

IV. *inp2cpa*: A Tool for Rapid Integration

A. *inp2cpa Basic Functionalities*

As mentioned, the epanetCPA toolkit requires an engineer to have knowledge on how to extract relevant data from .inp files and use that information to create .cpa files. Learning these file types and their syntax can be difficult and time consuming to correctly implement for those without experience with relevant field-specific programs, as well as the toolkits themselves. To make these toolkits more accessible we have taken and extended the functionalities of the tool *inp2cpa*, created by Nikolopuolos [11], [22] and the EU STOP-IT team, to drastically reduce the time it takes to run bulk test simulations as well as create custom cyber-physical attacks to simulate on a water network. This tool is a python-based program that utilizes the WNTR toolkit [23]. WNTR is a python package created by the EPA and Sandia Labs to evaluate drinking water systems for water quality and resilience against damgage cause by demand, natural disasters, and cyber attacks. WNTR is capable of generating water network models, modifying network structure, evaluating disruptive events, simulating pressure driven and demand driven hydraulics. It is used by engineers in the infrastructure industry as well as other cybersecurity researchers around the world. *inp2cpa* uses

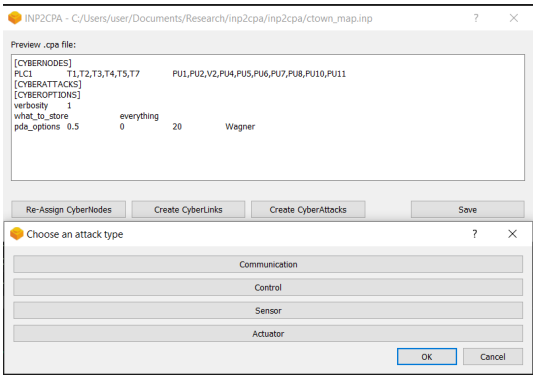

Fig. 4. *inp2cpa* Base Menu and Attack Selection Window

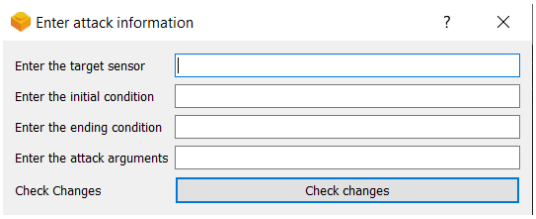

Fig. 5. *inp2cpa* Sensor Attack Specification Window

WNTRs file parsing capabilities in its network.controls script to build a python dictionary using the control section of .inp files. With this dictionary *inp2cpa* autmoatically generates a basic .cpa file. We have expanded *inp2cpa* to allow users to modify the automatically generated cyber-attack file by adding Cyberlinks and Cyberattacks. A Cyberlink is a way that a user can show how their hardware is connected. For example, if a series of actuators where connected to one plc, a user could add cyberlinks to the .cpa show the link between each actuator and its plc and then the plc to its SCADA system. Adding these links will allow the user to simulate attacks that take advantage of or disrupt those connections. The user can now add four types of cyber-attacks:

- *Communication* - intercepting and replacing communications between hardware
- *Control* - Changing the control logic of how physical components operate
- *Sensor* - manipulates the values sent out by sensors
- *Actuator* - take control of a physical component (e.g. valves, pumps) and manipulate it

We have simplified the process of creating these attacks by getting key information like the names of the sensor to be attacked and what values the want to interject into that sensor and then using string manipulation and concatenation we add it to a .cpa file with the correct syntax (as specified in Munteanu et al. [24]) and create an attack file ready for use. *inp2cpa* is meant to be used specifically with epanetCPA, and our contribution has expanded on the original automated processing of controls by completing several of the originally-proposed features, including customization and control menus, as well as numerous fixes to the text-parsing and error-checking features of the original code. We intend, however to make it compatible with DHALSIM as well by adding YAML, "Yet Another MarkUp language", used for DHALSIM configuration files, as an output, along with potentially other languages for file conversion and creation.

B. *inp2cpa: Resiliency Checking On-the-Fly*

In order to allow in-application review of the user's networks against common network resiliency metrics, *inp2cpa* creates a *G(V,E)* graph theory model of the network as defined by the user, using the general form of:

$$G\{Nd, Ln\}$$
$$Nd\{S, A, Con\}$$
$$Ln\{So, De, S\}$$

```
[CONTROLS]
LINK    WWT0FCV0001 120.000000 If Node WWT0TK0001 Below 5.500000
LINK    WWT0FCV0001 Closed If Node WWT0TK0001 Above 8.500000
LINK    WWT0PMP0101 Open If Node WWT0TK0002 Below 5.500000
LINK    WWT0PMP0101 Closed If Node WWT0TK0002 Above 8.500000
```

Fig. 6. Control section of an .inp file

```
[CYBERNODES]
; Name, Sensors, Actuators
PLCT1,  P_WWT0TK0001,
PLCFCV, F_WWT0FCV0001 S_WWT0FCV0001, WWT0FCV0001
PLCPMP, F_WWT0PMP0101 S_WWT0PMP0101, WWT0PMP0101
PLCT2, P_WWT0TK0002,
; SCADA


[CYBERLINKS]
; Source,Destination,Sensors
PLCT1, SCADA, P_WWT0TK0001
PLCT1, PLCFCV, P_WWT0TK0001
PLCT2, SCADA, P_WWT0TK0002
PLCT2, PLCFCV, P_WWT0TK0002
PLCT1, PLCPMP, P_WWT0TK0001
PLCT2, PLCPMP, P_WWT0TK0002
PLCFCV, SCADA, F_WWT0FCV0001 S_WWT0FCV0001
PLCPMP, SCADA, F_WWT0PMP0101 S_WWT0PMP0101


[CYBERATTACKS]
; Type,Target,Init_cond,End_cond,Arguments
; Attack on communication link between TK1 water level sensor and PLC1 (
; device, leading to forcible shutdown and continuous drain of the tank
Communication, NULL-P_WWT0TK0001-PLCT1, TIME==10, TIME==20, constant 8.6
```

Fig. 7. Post-processing of Fig. 4 within *inp2cpa*, resulting .cpa file, including user-specified attack against communication link.

, wherein a network graph is modeled by a graph G of nodes Nd and links Ln, each of which is represented by a set of tuples representing $Nd\{\boldsymbol{S}ensors, \boldsymbol{A}ctuators, \boldsymbol{Con}trols\}$ and $Ln\{\boldsymbol{So}urce, \boldsymbol{De}stination, \boldsymbol{S}ensors\}$. Utilizing this approach, a number of network resiliency metrics can be tested against, to give immediate feedback to users on their network's likely resilience against disruption and/or malicious activity. As a case study for this, we utilized automatic input of the common hydraulic simulation baseline of the *ctown* model alongside user-defined custom nodes and links, extracting a subset of the hydraulic network representing the control nodes PLC1 and PLC2, responsible for respectively: monitoring pump flow and junction pressure on the first three pumps in the network; monitoring water reserve tank level for the corresponding pumped reserve tank. This subset of the overall network represents just under half of the overall network capacity and complexity, and can be seen in in Fig.8 However, while it represents a high level of physical complexity, the logical complexity is often significantly lower. As shown in Taormina et al. [19] in their cybernode and link layouts for the ctown attack scenarios, a common way this might be handled is simply by assigning one PLC to monitor tank levels and separately, one to control the pumps feeding the network and monitor pressure levels on either side of the pumps for potential issues. However, as demonstrated by their own attack simulations against this set of control components, such a simple design has effectively no resiliency against any attack which interrupts or replaces valid communication between components, nor did they attempt to quantify or otherwise assess the resilience of cyber components of the network.

The results of this attack as simulated in Fig. 9 show that even interrupting one communication link between the sensor-monitoring PLC and the pump-controlling PLC will result in the system being entirely unable to identify and respond to conditions in the tank. While pumps should have been disconnected at $\tilde{5}8$ hours, the pumps continue to run and create overflow. Either duplicate tracking on the relevant sensor by the pump PLC or additional nodes (for example, a SCADA unit) tracking and sending data to nodes waiting on information would have resolved this, but the total lack of either results in likely damage to the system. While total duplication and redundancy across all nodes and controls in a network is impractical financially, and introduces both considerable extra complexity and potential additional surface area for attackers to target, we believe that even a small amount of additional connectivity and built-in resiliency in design would contribute significant value here, if only by ensuring that multiple attacks or interruptions would need to occur simultaneously to guarantee significant impact on the system.

In addressing this gap, we utilized the aforementioned graph theory model [25]–[27] alongside the findings of Alenazi et al. [28], in which Total Graph Diversity (TGD) 1 was identified across multiple structured and random network designs to be the most effective predictor of network resiliency against outages and directed attacks, to evaluate different configurations of the cyber-physical network. This metric, which is first described in Rohrer et al. [29] is measured as the average of Effective Path Diversity (EPD) 2, representing lowest path

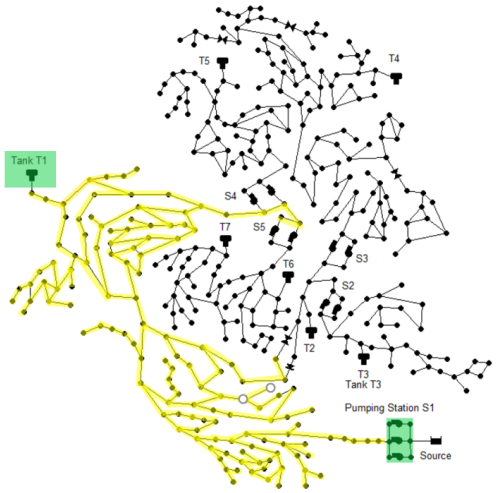

Fig. 8. Subsection of CTown Relevant to DoS Attack

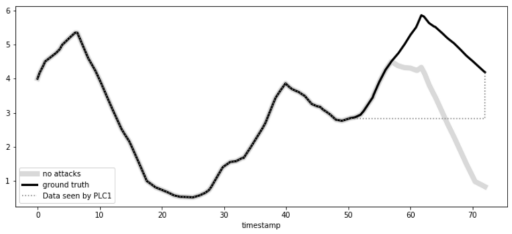

Fig. 9. Denial-of-Service Attack against PLC-monitored tank system

diversity 1 over a set of paths through the network, in this case over the directed edge links from node to node. Path diversity is determined for any given path among a set of possible paths between two nodes by a simple equation evaluating path length against shortest possible path length. EPD additionally factors in a λ value which is decided upon for any given network based on experimentation and desired outcomes. As a result of the exponential nature of the EPD formula, greater λ values correlate with a reduced impact of K_{sd} (minimum path diversity between two points in a graph 3) values on the outcome, indicating reduced gains on resiliency for additional path diversity. Pseudocode for a simple implementation of each can be found in 1 and 2.

$$D(P_a, P_b) = 1 - \frac{|P_a \oplus P_b|}{|P_b|} \tag{1}$$

$$EPD(P_a, P_b) = 1 - \exp^{-\lambda * K_{sd}} \tag{2}$$

$$K_{sd} = \sum_{i=1}^{k} D_{min}(P_i) \tag{3}$$

For the purpose of our example resilient system graphs, we will utilize the same subsection of physical network, and the same base logical layout, building out connectivity and creating duplication to showcase how TGD can be used to identify maximum resiliency gains for minimal additional infrastructure and complexity. Three values of λ, $\{0.2, 1, 5\}$, will be tested to demonstrate the impact they have on resiliency

Algorithm 1 TGD($Graph$):

```
sum ← 0
cnt ← 0
for node_s in Graph do
    for node_d in (Graph − node_s) do
        cnt ← cnt + 1
        sum ← sum + EPD(Graph, node_s, node_d)
    end for
end for
return sum/cnt
```

Algorithm 2 EPD($Graph, node_s, node_d$):

```
if Graph contains node_s, node_d then
    K_sd ← 0
    best ← []
    p0 = ShortestPath(Graph, node_S, node_D) [1]
    for path in AllPaths(Graph, node_S, node_D) do [2]
        if path ≠ p0 and 1 − size(p0⊕path))/size(path) > t_k_sd then
            best = path
            if size(best) == 0 then        ▷ Path diversity is 0
                k_sd ← 0
            else
                k_sd ← 1 − size(p0⊕best))/size(best) > t_k_sd
            end if
        end if
    end for
    return 1 − exp^{−λ∗K_sd}
else
    return 0        ▷ One or more nodes DNE in network.
end if
```

▷ [1, 2] As both ShortestPath and AllPaths are well-known graph theory algorithms which have numerous possible implementations, we note that any of the commonly-used approaches can be applied to this problem.

scores as nodes are added and connectivity increased. The base network scenario with limited connectivity, a fully-connected variation, and two variations on the network with a duplicate tracker on the tank level sensor were run through TGD checking, with the results shown in Table 1 below.

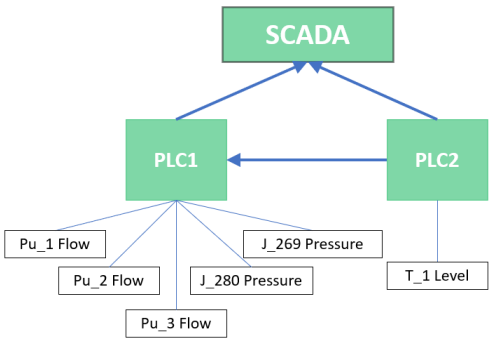

Fig. 10. Base Logical Model

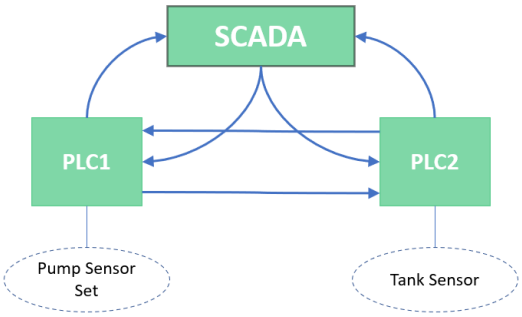

Fig. 11. Bidirectional Communication and Checking

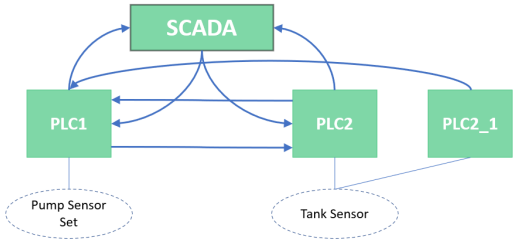

Fig. 12. Single Duplication on Tank Level, Partial Connection

TGD Values by Topology and λ			
λ	0.2	1	5
Fig. 10	0.0208	0.0811	0.16072
Fig. 11	0.12482	0.48658	0.96432
Fig. 12	0.08364	0.33249	0.70274
Fig. 13	0.09516	0.39347	0.91791

You can see that TGD weights heavily on interconnectivity, encouraging two-way communication and checking between cyber nodes. At all λ values, it rewards additional connectivity, and penalizes where the number and directness of paths are limited, although additional connectivity is much more heavily rewarded for higher levels of λ. It can be seen that simply adding a handful of connections to the base logical model, predicted resiliency (correlated with TGD) can be greatly improved. However, we must also note the severe penalization for the additional duplicate node when said node is not fully connected– this is not reflective of the likely effect on resiliency, since resiliency should not be negatively impacted by the addition of backup/duplicate sources and checks. This

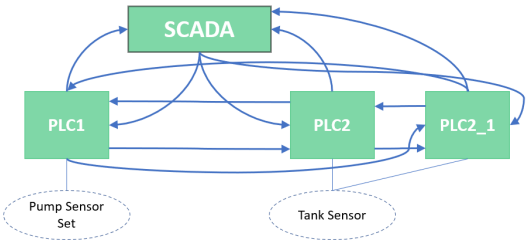

Fig. 13. Single Duplication on Tank Level, Full Connection

indicates that while TGD can be tested for networks in development and used to estimate relative resilience, additional metrics should be tested and integrated in future releases of *inp2cpa* and any future publications. Nevertheless, resiliency metrics like this are relevant to both standard communication and critical infrastructure control systems networks, and this additionally allows users an initial assessment of the likely resiliency of their network before lengthy simulations and tests are applied.

V. Conclusion and Future Work

The extended functionalities of the tool *inp2cpa* drastically reduces the time it takes to create and run bulk test simulations, as well as enabling technicians and engineers to create custom cyber-physical attacks to simulate on a water network and investigate the impact of the attack. This will be beneficial to engineers and technicians who work with critical infrastructure but do not have the necessary programming experience to efficiently use EPANET and epanetCPA. Future additions will include features and functionality to expand this to include DHALSIM configuration and attack scenario creation, along with a deeper dive into relevant existing resiliency metrics, and potential development of custom resiliency metrics for cyber-physical and smart-device systems based on their unique characteristics. We plan to continue to add to *inp2cpa* to make it as useful as possible to technicians and engineers in the industry. We are currently laying the ground work to add YAML functionality, and are also considering adding python configuration and device file generation, and will consult with members of industry and technical experts to identify what they would see as the most potentially useful additions to any such tool aiming to provide utility and create ease-of-access to simulation and verification toolkits. We believe one of the best ways to move forward with this tool is to eventually migrate it from a guided file creation tool to a fully automated file converter. While some components, such as cyberlinks, cannot be inferred by us and require user input we believe most other functions can be at least in-part, if not fully, automated. Eventually we would also like to see this tool, or core automated components of it, integrated into a simulation toolkit like epanetCPA or DHALSIM. If we were able to integrate this tool with an existing simulation toolkit that would significantly improve the accessibility of that toolkit to technicians in industry and researchers looking to advance knowledge in the field. *inp2cpa*, and tools like it, will make securing critical infrastructure from cyber-physical threats quicker and easier.

Acknowledgment

This material is based upon work supported by the National Science Foundation Computer and Information Science and Engineering (CISE) devision, award number 1846493 of the Secure and Trustworthy Cyberspace (SaTC) program: Formal TOols foR SafEty aNd. Security of Industrial Control Systems (FORENSICS).

References

[1] (). "Year in review — dragos," [Online]. Available: https://www.dragos.com/year-in-review/ (visited on 08/10/2021).

[2] J. Slowik, "Evolution of ICS attacks and the prospects for future disruptive events," p. 15,

[3] J. P. •. Jun 7 and 2021. (Jun. 8, 2021). "Colonial pipeline cyberattack: Timeline and ransomware attack recovery details," MSSP Alert, [Online]. Available: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/ (visited on 09/26/2021).

[4] (). "Aurora: Homeland security's secret project to change how we think about cybersecurity," MuckRock, [Online]. Available: https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/ (visited on 09/26/2021).

[5] (). "Ukraine power cut 'was cyber-attack' - BBC news," [Online]. Available: https://www.bbc.com/news/technology-38573074 (visited on 08/27/2021).

[6] (). "Triton 2.0 and the future of OT cyberattacks," FutureIoT. Library Catalog: futureiot.tech, [Online]. Available: https://futureiot.tech/whitepaper/triton-2-0-and-the-future-of-ot-cyberattacks/ (visited on 08/05/2020).

[7] (). "Cybersecurity lessons utilities can learn from the oldsmar water plant hack," [Online]. Available: https://biztechmagazine.com/article/2021/04/cybersecurity-lessons-utilities-can-learn-oldsmar-water-plant-hack (visited on 07/13/2021).

[8] C. Cimpanu. (). "Two more cyber-attacks hit israel's water system," ZDNet. Library Catalog: www.zdnet.com, [Online]. Available: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/ (visited on 07/22/2020).

[9] M. D. Abrams, "Malicious control system cyber security attack case study–maroochy water services, australia," p. 16,

[10] K. E. Hemsley and D. R. E. Fisher, "History of industrial control system cyber incidents," INL/CON–18-44411-Rev002, 1505628, Dec. 31, 2018, INL/CON–18–44411–Rev002, 1 505 628. DOI: 10.2172/1505628. [Online]. Available: http://www.osti.gov/servlets/purl/1505628/ (visited on 07/02/2020).

[11] (). "Nikolopoulos, d. (2020). inp2cpa. in stop-it," [Online]. Available: http://tl.stop-it-project.eu/d/Tool/4.

[12] P.-N. Carron, L. Trueb, and B. Yersin, "High-fidelity simulation in the nonmedical domain: Practices and potential transferable competencies for the medical field," *Advances in medical education and practice*, vol. 2, p. 149, 2011.

[13] M. Barnett, D. Gatfield, and C. Pekcan, "A research agenda in maritime crew resource management.," English, in *Proceedings of the International Conference on Team Resource Management in the 21st Century*, Publisher: Embry-Riddle Aeronautical University., United States: Embry-Riddle Aeronautical University, 2003.

[14] R. Helmreich, J. Wilhelm, J. Klinect, and A. Merritt, *Improving teamwork in organizations*, 2001.

[15] C. Hetherington, R. Flin, and K. Mearns, "Safety in shipping: The human element," *Journal of Safety Research*, vol. 37, no. 4, pp. 401–411, 2006, ISSN: 0022-4375. DOI: https://doi.org/10.1016/j.jsr.2006.04.007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022437506000818.

[16] G. Alinier and A. Platt, "International overview of high-level simulation education initiatives in relation to critical care," *Nursing in Critical Care*, vol. 19, no. 1, pp. 42–49, 2014. DOI: https://doi.org/10.1111/nicc.12030. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/nicc.12030. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/nicc.12030.

[17] K. Bisw, *The international journal on advances in systems and measurements is published by IARIA. ISSN: 1942-261x*.

[18] A. Bounceur, "Cupcarbon: A new platform for designing and simulating smart-city and iot wireless sensor networks (sci-wsn)," in *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ser. ICC '16, Cambridge, United Kingdom: Association for Computing Machinery, 2016, ISBN: 9781450340632. DOI: 10.1145/2896387.2900336. [Online]. Available: https://doi.org/10.1145/2896387.2900336.

[19] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *Journal of Water Resources Planning and Management*, vol. 143, no. 5, p. 04 017 009, 2017.

[20] A. Murillo, R. Taormina, N. Tippenhauer, and S. Galelli, "Co-simulating physical processes and network data for high-fidelity cyber-security experiments," in *Sixth Annual Industrial Control System Security (ICSS) Workshop*, Austin TX USA: ACM, Dec. 8, 2020, pp. 13–20, ISBN: 978-1-4503-9002-6. DOI: 10.1145/3442144.3442147. [Online]. Available: https://dl.acm.org/doi/10.1145/3442144.3442147 (visited on 05/20/2021).

[21] ——, "Co-simulating physical processes and network data for high-fidelity cyber-security experiments," in *Sixth Annual Industrial Control System Security (ICSS) Workshop*, 2020, pp. 13–20.

[22] D. Nikolopoulos, G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, and C. Makropoulos, "Cyber-physical stress-testing platform for water distribution networks," *Journal of Environmental Engineering*, vol. 146, no. 7, p. 04 020 061, Jul. 2020, ISSN: 0733-9372, 1943-7870. DOI: 10.1061/(ASCE)EE.1943-7870.0001722. [Online]. Available: http://ascelibrary.org/doi/10.1061/%28ASCE%29EE.1943-7870.0001722 (visited on 07/17/2020).

[23] K. A. Klise, R. Murray, and T. Haxton, "An overview of the water network tool for resilience (wntr).," 2018.

[24] R. Taormina, S. Galelli, H. Douglas, N. Tippenhauer, E. Salomons, and A. Ostfeld, "A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems," *Environmental Modelling & Software*, vol. 112, pp. 46–51, 2019, ISSN: 1364-8152. DOI: https://doi.org/10.1016/j.envsoft.2018.11.008.

[25] H. Mehrpouyan, D. C. Jensen, C. Hoyle, I. Y. Tumer, and T. Kurtoglu, "A model-based failure identification and propagation framework for conceptual design of complex systems," in *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, vol. 45011, 2012, pp. 1087–1096.

[26] H. Mehrpouyan, B. Haley, A. Dong, I. Y. Tumer, and C. Hoyle, "Resiliency analysis for complex engineered system design," *AI EDAM*, vol. 29, no. 1, pp. 93–108, 2015.

[27] H. Mehrpouyan, B. Haley, A. Dong, I. Y. Tumer, and C. Hoyle, "Resilient design of complex engineered systems against cascading failure," in *ASME International Mechanical Engineering Congress and Exposition*, American Society of Mechanical Engineers, vol. 56413, 2013, V012T13A063.

[28] M. Alenazi and J. Sterbenz, "Evaluation and comparison of several graph robustness metrics to improve network resilience," Oct. 2015, pp. 7–13. DOI: 10.1109/RNDM.2015.7324302.

[29] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification for future internet end-to-end resilience and survivability," *Telecommunication Systems*, vol. 56, no. 1, pp. 49–67, May 2014, ISSN: 1018-4864, 1572-9451. DOI: 10.1007/s11235-013-9818-7. [Online]. Available: http://link.springer.com/10.1007/s11235-013-9818-7 (visited on 11/29/2021).