environmental sciences proceedings

MDPI

Proceeding Paper

Assessing Cyber-Physical Threats under Water Demand Uncertainty †

Georgios Moraitis [1,*], Ioannis Tsoukalas [1], Panagiotis Kossieris [1], Dionysios Nikolopoulos [1], George Karavokiros [1], Dimitrios Kalogeras [2] and Christos Makropoulos [1]

[1] Department of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical University of Athens, 15780 Athens, Greece
[2] Institute of Communication and Computer Systems, National Technical University of Athens, 15780 Athens, Greece
* Correspondence: georgemoraitis@central.ntua.gr; Tel.: +30-210-772-2816
† Presented at the International Conference EWaS5, Naples, Italy, 12–15 July 2022.

Abstract: This study presents an approach for the assessment of cyber-physical threats to water distribution networks under the prism of the uncertainty which stems from the variability and stochastic nature of nodal water demands. The proposed framework investigates a single threat scenario under a spectrum of synthetic, yet realistic, system states which are driven by an ensemble of stochastically generated nodal demands. This Monte Carlo-type experiment enables the probabilistic inference about model outputs, and hence the derivation of probabilistic estimates over consequences. The approach is showcased for a cyber-physical attack scenario against the monitoring and control system of a benchmark network.

Keywords: uncertainty; risk assessment; stochastic simulation; stochastic processes; cyber-physical threats; water demand; synthetic demand series; cyber-physical systems

check for updates

Citation: Moraitis, G.; Tsoukalas, I.; Kossieris, P.; Nikolopoulos, D.; Karavokiros, G.; Kalogeras, D.; Makropoulos, C. Assessing Cyber-Physical Threats under Water Demand Uncertainty. *Environ. Sci. Proc.* **2022**, *21*, 18. https://doi.org/10.3390/environsciproc2022021018

Academic Editors: Vasilis Kanakoudis, Maurizio Giugni, Evangelos Keramaris and Francesco De Paola

Published: 19 October 2022

1. Introduction

Urban water systems, as many other critical infrastructures, are undergoing a digital transformation which, evidently, yields both merits and perils [1,2]. Their long-established *modus operandi* is reshaped by the dynamic interconnection of cyber and physical processes and assets—progressively moving towards a new, cyber-physical systems' (CPS) architecture [3,4]. As recent incidents demonstrate [5], this increases the attack surface of the water systems and allows for emerging threats against the CPS, hindering the monitoring and control processes and compromising the integrity of the water supply—including potential weaponisation. As a result, traditional system thinking is challenged, while security planning becomes more intricate with the addition of a new component in risk assessment schemes, that of cyber-physical risks. The need for adjustment by the sector is reflected by an ever-increasing development of novel solutions, cyber-physical modelling platforms, techniques and frameworks to strengthen security and risk assessment at both conceptual and practical levels [6].

Contemporary risk assessment frame works for the water sector investigate the potential threats by adopting the typical scenario-based approach [7,8] to analyse, and subsequently evaluate the resulting failure through suitable metrics [9]. In the scenario-based approach, a set of external events drives a pre-defined system model to analyse risks—implying mutually that this model represents a usual state of the system. However, urban water systems are complex and dynamic in nature and can exhibit a notable variability in their behaviour, even under normal operating conditions. This poses questions on the representativeness of internal parameters that drive the system model, and hence the simulated outcomes, and the value of the resulting risk information, as uncertainty pertains the risk-relevant data from the deterministic model set-ups.

Uncertainty analysis has long been acknowledged as a pivotal concept for risk characterization [10], yet rarely addressed formally as a core component of risk assessment techniques or design practices. A paradigm shift is introduced formally by the International Organization for Standardization (ISO), which embeds the notion of *uncertainty* to the definition of risk, in reference to potential events and their consequences [11]. Moreover, in recent years, the appropriate characterization and handling of *uncertainty* is revisited, leading to the reshaping of traditional analytical tools [12] with the help of uncertainty propagation techniques. This includes stochastically-enhanced frameworks developed to systematically cope with uncertainties, inter alia in water pipe rehabilitation plans [13], flood defence infrastructure [14], long-term operation and resilience of urban water systems [15], etc. One such framework is also introduced for the assessment of cyber-physical risks against urban water systems [16] under the prism of, both epistemic and aleatory, uncertainties. An epistemic uncertainty, also known as systemic, is linked to the degree of factual knowledge (or lack thereof). On the other hand, an aleatory uncertainty refers to the inherent probabilistic variability of the underlying components.

This work focuses on the latter type, and specifically examines the assessment of cyber-physical threats under the uncertain and high variable nature of water demand, that is a key driver of urban water systems [17,18]. Specifically, we propose a framework that couples the sector's scenario-based approaches with state-of-the-art stochastic simulation approaches [19–21] that allow to assess a single threat scenario under a spectrum of stochastically generated demands, in a Monte Carlo-type experiment. This formulation allows the inference about the model's outputs, and related consequences, in probabilistic terms. The overall result is an uncertainty-informed, probabilistic estimation of the risk's severity.

The remaining of the paper showcasing the proposed stochastic assessment framework is organized on the basis of a demo water distribution network (WDN). In more detail, Section 2.1 provides information about the case study *per se*, Section 2.2 entails the methodology for the stochastic simulation/generation of water demand time series and Section 2.3 details the generation of cyber-physical threat scenarios for a WDN. Section 3 discusses the approach employed for the probabilistic assessment of threat scenarios. Finally, Section 4 concludes this work through a summary of its main findings and conclusions.

2. Stochastic Risk Assessment for WDN

2.1. The C-Town Case Study

C-town is an EPANET demo WDN, based on a medium-sized real world network [22]. It is comprised of seven tanks, and five pumping stations with a total of 11 head pumps, which are used to store and regulate the water distribution to 388 consumption nodes. The WDN is supplied by a single source, the R1 seasonal reservoir, with an average hourly production of approximately 613.17 m^3/h. The system is divided into five district metered areas (DMA), all of which include a pumping station and at least one tank in them, as illustrated in Figure 1. The fundamental C-Town operation mode draws water from R1 through the linked pumping station, according to the level of tank T1. In high water levels, only one pump draws water, and a second pump is activated for critically low levels. The pumping station also has a third, redundant pump placed in parallel. The flow from DMA1 to DMA2 is regulated with the use of two flow control valves that operate according to the T2 tank level, while two pressure regulating valves (PRV) are placed within DMA2. Water from T2 is pumped to the higher tanks, namely T3 and T4. The pumping stations of DMA4 and DMA5 pump water to tanks T5, T6 and T7 from DMA1 and T1. The pumping stations activation rules are based on the level sensors of their DMA tanks.

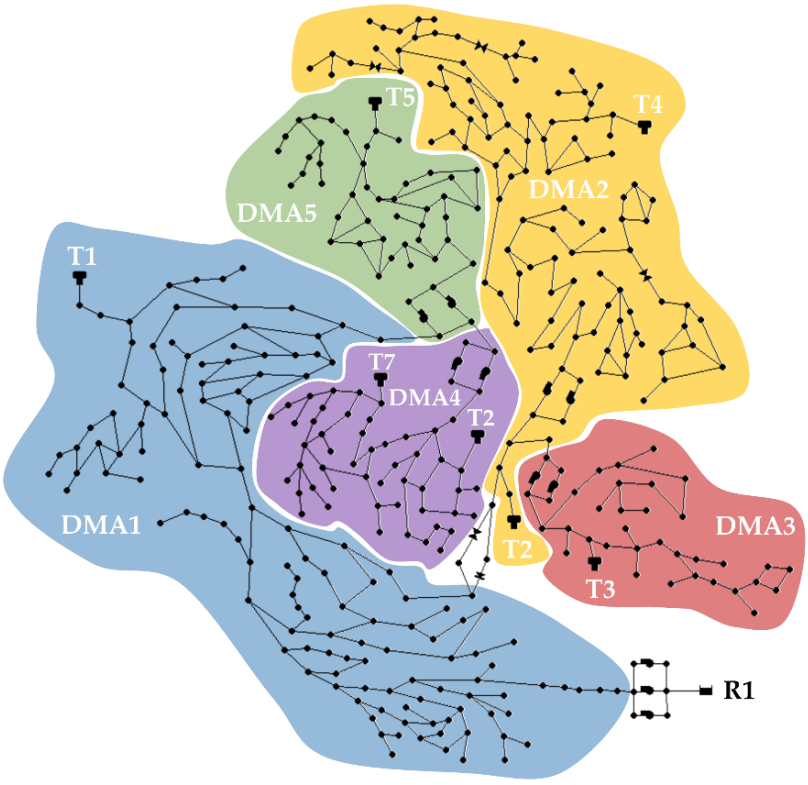

Figure 1. Visualization of the C-town WDN with five DMAs highlighted.

2.2. Generation of Synthetic Water Demand Series

In the design, analysis and management of urban water systems, the water demand, as a key driver of these systems, is analysed and modelled at different temporal and spatial levels, depending on the requirements and type of analysis under study. As the spatial and temporal resolution of the analysis is increasing, the level of uncertainty and randomness of the water demand increases too, posing extra challenges and difficulties. Specifically, at fine scales, water demand is characterised by intermittent behaviour (i.e., the presence of zero values in the series), deviation from Gaussianity, a variety of temporal and spatial dependence structures, and various types of seasonality [19]. The modelling of these peculiarities is feasible by studying the water demand on the basis of probabilistic notions and concepts, such as those of random variables and stochastic processes. This approach allows to generate a large number of synthetic, yet statistically and stochastically consistent, water demand timeseries that can be employed as non-deterministic inputs to provide the system's responses under different scenarios—essentially, the approach adopted in this study.

Here, we treat as stochastic process the demand multiplier pattern used by the Epanet modelling approach to represent the variability of the customer's (nodal's) demand over time. The pattern is multiplied by a base demand assigned to each node in order to reproduce the actual size of the variability, along with the peak and minimum demand periods throughout the simulation horizon. The C-Town case study comes along with a set of five demand multiplier patterns (one for each DMA), with an hourly temporal resolution, that span over an entire week, to describe the overall system's demand processes [22].

To generate synthetic water demand multiplier patterns, the anySim R package [20] was employed. This package provides state-of-the-art stochastic simulation methods that allow the exact preservation of any marginal distribution and any dependence structure of the stochastic processes under study [23–25]. In a nutshell, the method implemented herein is based on the coupling of Nataf's joint distribution model (i.e., the Gaussian copula) with the widely known class of linear stochastic models. According to Nataf's joint distribution model, the joint distribution of random variables with any target arbitrary

marginal distributions can be obtained by mapping an auxiliary multivariate standard Gaussian distribution via the inverse cumulative distribution functions (ICDFs). The implemented methods utilize the link between correlation coefficients in the Gaussian and the target domain, also reproducing the target correlations. Moving to the stochastic process simulation, *anySim* employs a similar concept that is based on the mapping (through the ICDF) of an auxiliary Gaussian process (Gp) through the ICDF, to establish processes with the target marginal distribution and correlation structure. Specifically, herein we employed the Gamma distribution to model the marginal behaviour of the demand multiplier patterns of all five DMAs [26], while the classical autoregressive model (AR(p)) was employed as an underlying linear model to reproduce the auto-correlation structure of each pattern and the lag-0 cross-correlation between the patterns. To cope with seasonality, the given hourly demand multiplier patterns were first standardised over the mean, and hence the stochastic simulation was performed under the assumption of stationarity. The generated series were de-transformed via the inverse procedure to formulate the synthetic seasonally varying series that were used as inputs in EPANET.

Water demand series and their stochasticity have a significant influence over the dynamics of water systems in both short- (including instantaneous) and long-term horizons. Thus, despite the original pattern series having a 1-week duration, this work expands their duration to 2 weeks. This enables the full development of stochasticity in the system states under which the potential attack takes place (in the first week) and monitors the system's behaviour after the attack (during the second week) for any cascading effect of the cyber-physical threat.

Thus, the overall result of this step is a set of 500 (100 for each DMA, also preserving the lag-0 cross-correlation between them) synthetic hourly demand pattern timeseries for C-Town, each having a duration of 2 weeks. Figure 2 illustrates the median and outer bands of the 100 synthetic hourly demand patterns generated for DMA1. This stochastically generated ensemble is then introduced to the WDN model of C-Town, to derive a spectrum of stochastic, yet realistic system states, any of which can exist when an attack occurs.

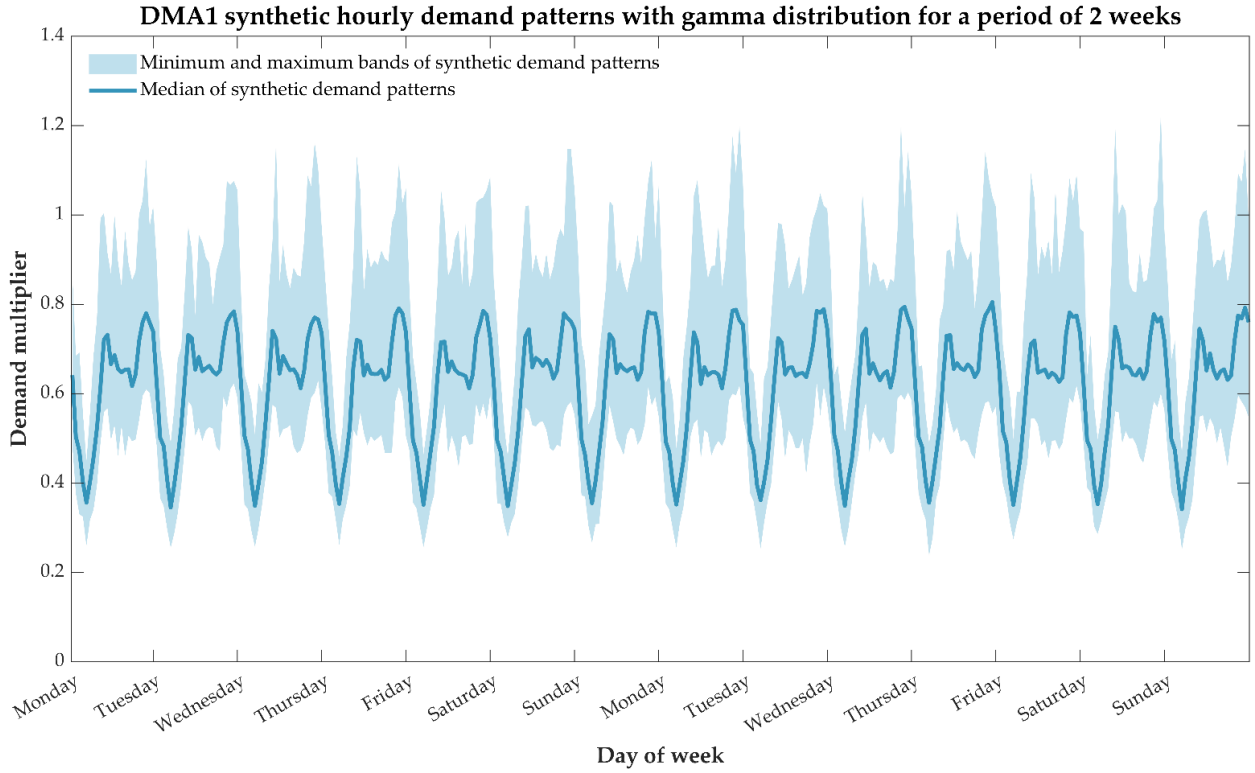

Figure 2. Median and outer bands (minimum and maximum) of the synthetic hourly demand pattern timeseries with gamma distribution generated for DMA1.

2.3. Threat Scenario and Risk Analysis

In a scenario-based risk assessment, the scenario is typically composed of a basic model of the system under common hydraulic conditions and a set of threats against assets of the water system. As a guiding tool to explore and identify potential cyber-physical threats against their systems, water utilities can utilize potential hazard databases either corporate, embedded in risk assessment toolkits, or found online.

In this study, we formulate an attack scenario against the monitoring and control system of C-Town, by targeting a tank's water level sensor. The attacker hijacks the connection between the T1 sensor and the PLC, overseen by the SCADA, and inserts bogus information. The false signal leads the system to believe that T1 is at high level, and the subsequent action is to turn off the pumping station at the reservoir R1. This shut down may lead to (some or even all) tanks in the system to empty, resulting in water supply deficiencies in the DMAs. The attack starts at 00:00 of the 8th day in the simulation and lasts for 24 h.

The described threat is transcribed in an EPANET-based threat scenario utilizing the capabilities of RISKNOUGHT [27,28]. It is a stress-testing platform, capable of simulating complex cyber-physical water systems with an emphasis on the resilience assessment in terms of both hydraulic and water quality dimensions. More specifically, RISKNOUGHT is used to formulate and run (a) the deterministic attack scenario using the default C-Town patterns and hydraulic states and (b) the ensemble of 100 attack scenarios (i.e., in a Monte Carlo fashion) using the stochastically generated patterns per DMA, which also affect the hydraulic state prior to the attack. The modelling is supported by the implementation of Pressure Driven Analysis (PDA) to realistically simulate hydraulic failure conditions and more specifically, under the Wagner approach [29].

3. Probabilistic Assessment of the Threat Scenario

The deterministic assessment of the above-described cyber-physical attack scenario, results in a total of 10,295 m^3 for the unmet demand metric (UD). Following the proposed stochastic risk assessment, the risk assessor produces an ensemble of 100 different realizations and hence, 100 different evaluations of the cyber-physical attack scenario. This allows the uncertainty-aware inference of the potential consequences, expressed probabilistically. The stochastic assessment of the potential consequences gives a median estimate of 10,805 m^3 of potential unmet demand. The related statistical properties are summarized in Table 1. Comparing the median value to that of the deterministic quantification, the values exhibit a difference of ~5%. However, the potential unmet demand can highly vary from these values. Exploring the empirical distribution of the resulting metrics, the upper level, estimated using the 95th percentile, is 12,620 m^3 and approximately 22.58% higher than the deterministic estimation. Moreover, the lower level, estimated for the 5th percentile, is 9542 m^3 and is approximately 7.88% lower than the deterministic value.

Table 1. Statistical characteristics of the unmet demand metric for the ensemble of 100 stochastically driven scenarios against C-Town.

	Median	Mean	Max	Min	Range	St. dev.	95th Percentile	5th Percentile
Unmet Demand (m^3)	10,805.33	10,999.58	13,617.59	8495.15	5122.43	962.85	12,620.23	9542.48

There is significant fluctuation in the UD metric, which is a consequence of the hydraulic variability of the WDN at the time of attack. The development of 1-week (i.e., prior to the attack) stochastic demand patterns yields a range of potential system states, i.e., tank levels, valve and pump statuses, nodal pressures, etc. As presented in Figure 3, there is strong negative correlation between the T1 tank water level and the total unmet demand for the 1-week period after the attack. This is expected, as the T1 influences the most important controls of the system related to the reservoir outflow, and in addition it is the targeted infrastructure in the scenarios.

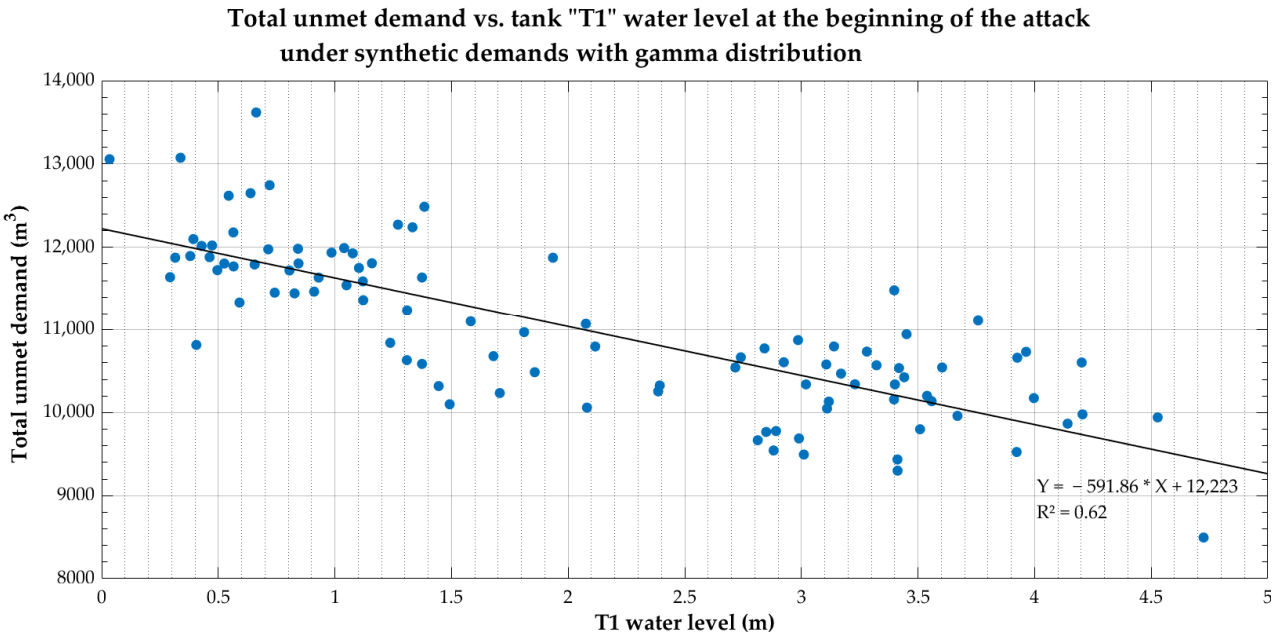

Figure 3. Relationship between the water level in tank "T1" when the cyber-physical attack starts and the resulting total unmet demand, simulated using synthetic hourly demand patterns with a gamma distribution.

4. Conclusions

The deterministic assessment of threat scenarios can provide a quick estimation for the outcome of an event and its order of magnitude, assuming a typical state of the WDN. Yet, it is argued that deterministic assessments of risks under "average conditions" misinterpret or even ignore key drivers that affect the extent of an outcome, such as the demand variability. To account for such inherent uncertainties, this work proposes risk assessors to incorporate stochastically generated demands in the scenario-based risk assessment scheme. To showcase the stochastic risk assessment approach, a single threat scenario was simulated under a spectrum of synthetic, yet realistic, system states, driven by the ensemble of stochastically generated nodal demands. This Monte Carlo-type experiment was used to probabilistically assess the WDN model outputs, and hence derived a probabilistic estimate over the severity of the threat scenario. As indicated by the results, the deterministic risk assessment approach underestimated the potential severity of a threat. This can greatly affect their prioritization against other, less severe events, leading overall to sub-optimal resilience and security strategies for a water system.

Author Contributions: Conceptualization, G.M. and D.N.; methodology, G.M., I.T., P.K. and D.N.; software, G.M., I.T., P.K., D.N. and G.K.; validation, I.T., P.K. and C.M.; formal analysis, D.N. and P.K.; investigation, G.M.; resources, G.K., D.K. and C.M.; data curation, D.N., I.T. and P.K.; writing—original draft preparation, G.M.; writing—review and editing, G.M., I.T., P.K. and D.N.; visualization, G.M.; supervision, D.K. and C.M.; project administration, G.M., D.K. and C.M.; funding acquisition, C.M. All authors have read and agreed to the published version of the manuscript.

Funding: The research work was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "First Call for H.F.R.I. Research" Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant (Project Number: HFRI-FM17-2918).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of the data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Savić, D. Digital water developments and lessons learned from automation in the car and aircraft industries. *Engineering* **2022**, *9*, 35–41. [CrossRef]
2. Sarni, W.; White, C.; Webb, R.; Cross, K.; Glotzbach, R. *Digital Water: Industry Leaders Chart the Transformation Journey*; International Water Association: London, UK, 2019.
3. Lee, J.; Bagheri, B.; Kao, H.-A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
4. Loukas, G. A Cyber-Physical World. In *Cyber-Physical Attacks*; Elsevier Science: Amsterdam, The Netherlands, 2015; pp. 1–19. [CrossRef]
5. Hassanzadeh, A.; Rasekh, A.; Galelli, S.; Aghashahi, M.; Taormina, R.; Ostfeld, A.; Banks, M.K. A Review of Cybersecurity Incidents in the Water Sector. *J. Environ. Eng.* **2020**, *146*, 03120003. [CrossRef]
6. Makropoulos, C.; Savić, D.A. Urban hydroinformatics: Past, present and future. *Water* **2019**, *11*, 1959. [CrossRef]
7. American Water Works Association. *Risk and Resilience Management of Water and Wastewater Systems. AWWA J100-10 (R13)*, 1st ed.; American Water Works Association US: Denver, CO, USA, 2010; ISBN 9781583217887.
8. Nikolopoulos, D.; Moraitis, G.; Makropoulos, C. 7. Strategic and Tactical Cyber-Physical Security for Critical Water Infrastructures. In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*; Soldatos, J., Praça, I., Jovanovic, A., Eds.; Now Publishers: Delft, The Netherlands, 2021; pp. 159–187. ISBN 978-1-68083-823-7.
9. Moraitis, G.; Nikolopoulos, D.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. *J. Environ. Eng.* **2020**, *146*, 04020108. [CrossRef]
10. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res.* **2016**, *253*, 1–13. [CrossRef]
11. ISO. *ISO 31000 Risk Management—Principles and Guidelines*; International Organization for Standardization: London, UK, 2018.
12. Klinke, A.; Renn, O. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Anal.* **2002**, *22*, 1071–1094. [CrossRef] [PubMed]
13. Savic, D.A. Coping with risk and uncertainty in urban water infrastructure rehabilitation planning. In Proceedings of the Acqua e Citta- I Convegno Nazionale di Idraulica Urbana, S'Agnello 2005, Napoli, Italy, 28–30 September 2005; Centro Studi Idraulica Urbana: Brescia, Italy, 2005.
14. Efstratiadis, A.; Dimas, P.; Pouliasis, G.; Tsoukalas, I.; Kossieris, P.; Bellos, V.; Sakki, G.; Makropoulos, C.; Michas, S. Revisiting Flood Hazard Assessment Practices under a Hybrid Stochastic Simulation Framework. *Water* **2022**, *14*, 457. [CrossRef]
15. Nikolopoulos, D.; Kossieris, P.; Tsoukalas, I.; Makropoulos, C. Stress-Testing Framework for Urban Water Systems: A Source to Tap Approach for Stochastic Resilience Assessment. *Water* **2022**, *14*, 154. [CrossRef]
16. Moraitis, G.; Nikolopoulos, D.; Koutiva, I.; Tsoukalas, I.; Karavokyros, G.; Makropoulos, C. The PROCRUSTES testbed: Tackling cyber-physical risk for water systems. In *Proceedings of the EGU General Assembly 2021*; EGU: Munich, Germany, 2021; p. EGU21-14903. [CrossRef]
17. Bao, Y.; Mays, L.W. Model for Water Distribution System Reliability. *J. Hydraul. Eng.* **1990**, *116*, 1119–1137. [CrossRef]
18. Walski, M.T.; Chase, D.V.; Savic, D.A.; Grayman, W.; Beckwith, S.; Koelle, E. *Advanced Water Distribution Modeling and Management*, 1st ed.; Haestead Press: Sydney, Australia, 2003; ISBN 0971414122.
19. Kossieris, P.; Tsoukalas, I.; Makropoulos, C.; Savic, D. Simulating Marginal and Dependence Behaviour of Water Demand Processes at Any Fine Time Scale. *Water* **2019**, *11*, 885. [CrossRef]
20. Tsoukalas, I.; Kossieris, P.; Makropoulos, C. Simulation of Non-Gaussian Correlated Random Variables, Stochastic Processes and Random Fields: Introducing the anySim R-Package for Environmental Applications and Beyond. *Water* **2020**, *12*, 1645. [CrossRef]
21. Kossieris, P.S. Multi-Scale Stochastic Analysis and Modelling of Residential Water Demand Processes. Ph.D. Thesis, National Technical University of Athens, School of Civil Engineering, Athens, Greece, 2020; 350p.
22. Ostfeld, A.; Salomons, E.; Ormsbee, L.; Uber, J.G.; Bros, C.M.; Kalungi, P.; Burd, R.; Zazula-Coetzee, B.; Belrain, T.; Kang, D.; et al. Battle of the Water Calibration Networks. *J. Water Resour. Plan. Manag.* **2012**, *138*, 523–532. [CrossRef]
23. Tsoukalas, I.; Efstratiadis, A.; Makropoulos, C. Building a puzzle to solve a riddle: A multi-scale disaggregation approach for multivariate stochastic processes with any marginal distribution and correlation structure. *J. Hydrol.* **2019**, *575*, 354–380. [CrossRef]
24. Tsoukalas, I.; Papalexiou, S.; Efstratiadis, A.; Makropoulos, C. A Cautionary Note on the Reproduction of Dependencies through Linear Stochastic Models with Non-Gaussian White Noise. *Water* **2018**, *10*, 771. [CrossRef]
25. Tsoukalas, I.; Makropoulos, C.; Koutsoyiannis, D. Simulation of stochastic processes exhibiting any-range dependence and arbitrary marginal distributions. *Water Resour. Res.* **2018**, *54*, 9484–9513. [CrossRef]
26. Kossieris, P.; Makropoulos, C. Exploring the Statistical and Distributional Properties of Residential Water Demand at Fine Time Scales. *Water* **2018**, *10*, 1481. [CrossRef]

27. Nikolopoulos, D.; Moraitis, G.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Cyber-Physical Stress-Testing Platform for Water Distribution Networks. *J. Environ. Eng.* **2020**, *146*, 04020061. [CrossRef]
28. Nikolopoulos, D.; Makropoulos, C. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water J.* **2022**, *19*, 256–270. [CrossRef]
29. Wagner, J.M.; Shamir, U.; Marks, D.H. Water Distribution Reliability: Simulation Methods. *J. Water Resour. Plan. Manag.* **1988**, *114*, 276–294. [CrossRef]