PROCRUSTES

The PROCRUSTES testbed: tackling cyber-physical risk for water systems

Georgios Moraitis[1], Dionysios Nikolopoulos[1], Ifigeneia Koutiva[1], Ioannis Tsoukalas[1], George Karavokiros[1], and Christos Makropoulos[1]

[1] School of Civil Engineering, National Technical University of Athens, Athens, Greece

EGU21-14903, EGU General Assembly 2021
https://doi.org/10.5194/egusphere-egu21-14903

[Session HS5.4.1]

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded 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)

Cyber-physical vectors in risk management

Contemporary urban water systems transform into **cyber-physical systems (CPS),** with increased attack surface and exposure to new threats from the cyber domain [1].

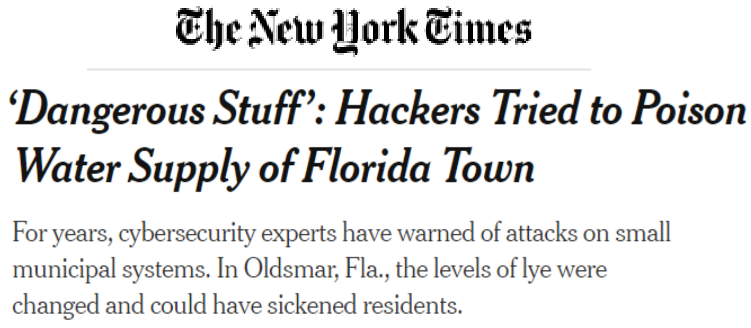
Motivated adversaries like disgruntled employees, organized hacker groups and state-affiliated actors target the water sector [2-5], seeking to exploit vulnerabilities and infringe upon the operational layers to compromise integrity.

A cyber-physical attack, could hone in on, at least, four different threat vectors [6-9]:

- chemical contamination,
- biological contamination,
- physical disruption and
- disruption of the supervisory and control systems.

And at different levels and escalation rates.

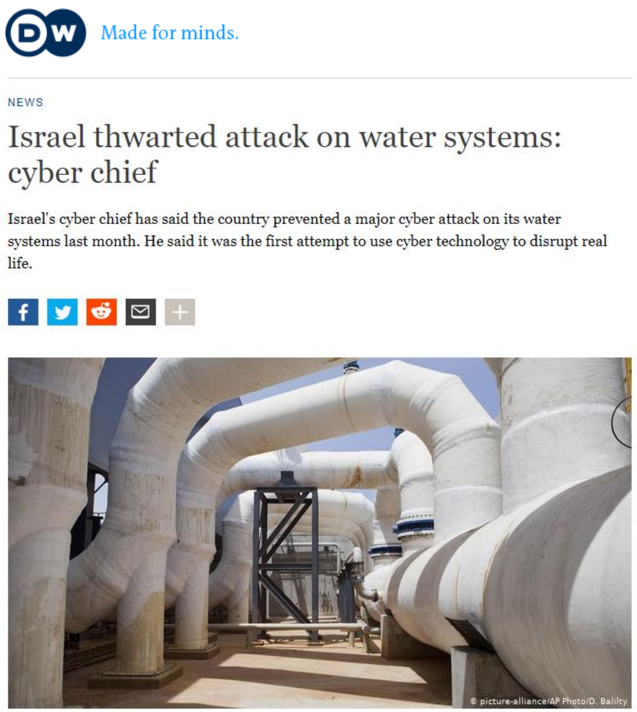
A successful attack resulting in consequences in one of these areas could cause major damage, including long periods of operational downtime, financial losses, loss of trust for water utilities and most importantly, **a direct threat to public health and societal stability**.



The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.



DW Made for minds.

NEWS

Israel thwarted attack on water systems: cyber chief

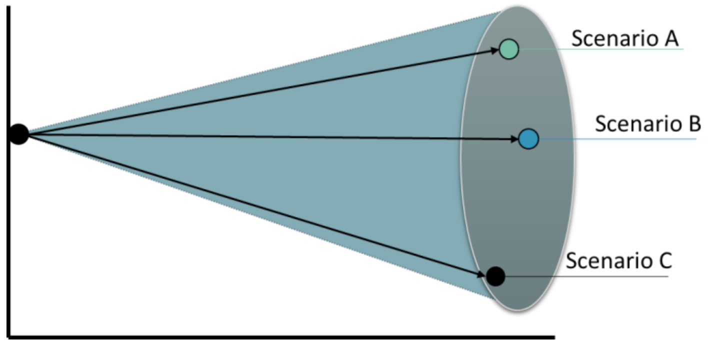
Israel's cyber chief has said the country prevented a major cyber attack on its water systems last month. He said it was the first attempt to use cyber technology to disrupt real life.

© picture-alliance/AP Photo/D. Balilty

It is no longer a matter of "*will* it happen?"; rather, it is a matter of "are we *well-prepared* for *when* it happens?"

Limitations and uncertainty in risk management

Despite operational intertwining of cyber and physical layers, the cybersecurity and operational risk management are still treated separately [10]. We need to develop tools and approaches that provide a **holistic**, **cyber-physical** view of **resilience** [11].



Impact →

Likelihood ↑	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

Deterministic single scenario

Common limitations:

- Attack records / statistical DBs are often **incomplete, biased or debased** [12,13], while expert judgment–based techniques for attack likelihood are susceptible to **misconceptions** over industrial **systems' security** [14]
- Most approaches lack the ability to characterize the **goal-driven behavioural rules** (e.g. target selection) and complex socio-technical structures (e.g. water CPS) [15-17].
- Threat scenarios are explored **deterministically** providing a limited view over the system's response against them. **Uncertainty** propagates to the estimated risk level magnitude and the resulting data-driven decisions.
- Existing solutions applied by large and ambitious utilities are not well known in the sector, and may not be easily **transferable or down-scalable to** Small and Medium-sized Utilities (**SMU**).

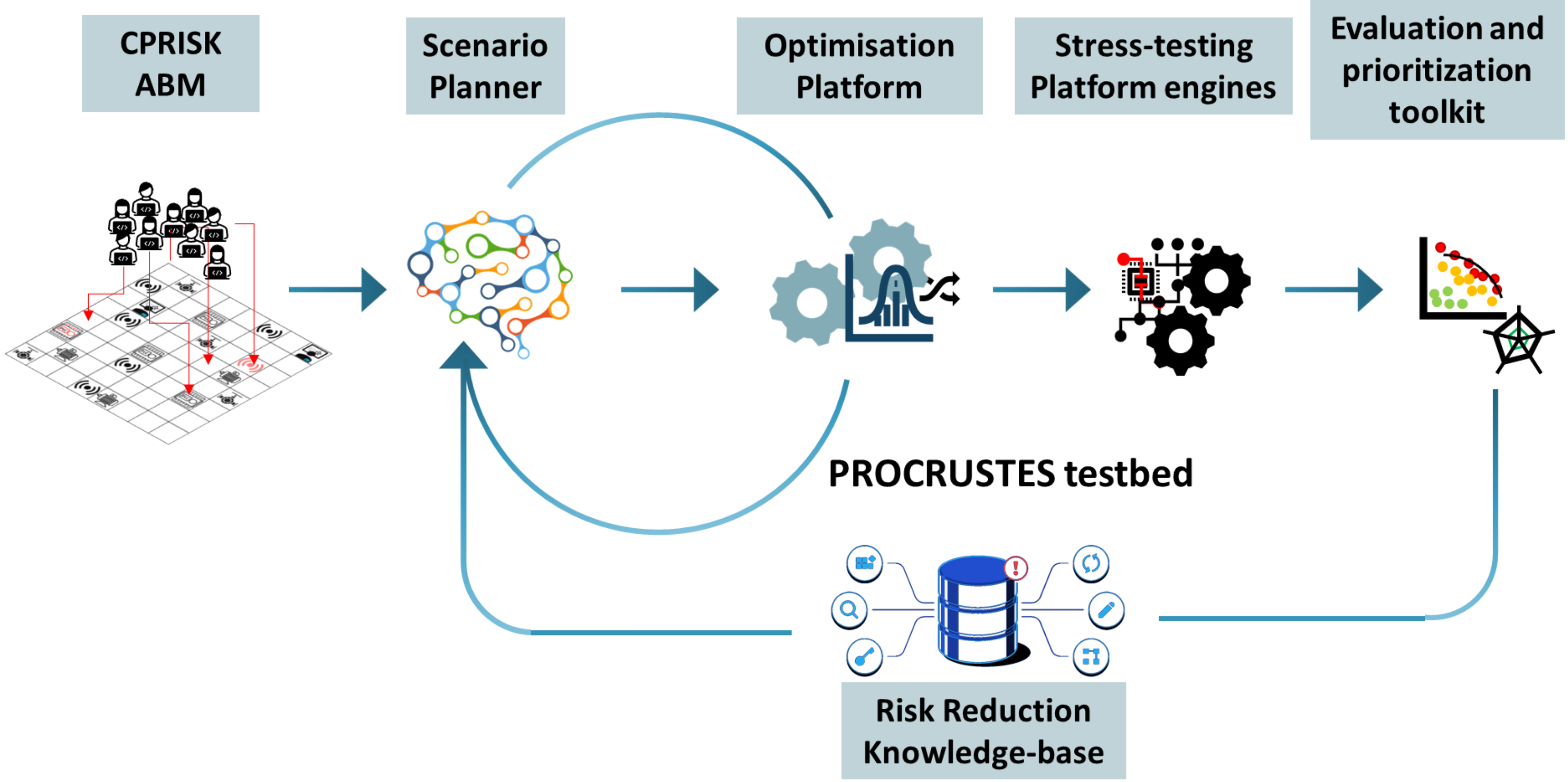
PROCRUSTES testbed

The PROCRUSTES project aspires to develop a combination of solutions and form a generic, unified process for combined cyber-physical resilience assessment under uncertainty, regardless of utility's size. At its core, the proposed **PROCRUSTES framework advances existing approaches** through:

a) an **Agent-Based Modelling (ABM) approach** to derive alternative routes to quantify risks considering the dynamics of socio-technical systems

b) an adaptable **optimisation platform** with **stochastic surrogate** timeseries generators and multivariate algorithms to assist **uncertainty analysis** and criticality prioritization

c) a **dynamic risk reduction knowledgebase (RRKB)** to facilitate the identification and selection of suitable measures and modify risks


CPRISK ABM
Scenario Planner
Optimisation Platform
Stress-testing Platform engines
Evaluation and prioritization toolkit
PROCRUSTES testbed
Risk Reduction Knowledge-base

Those solutions are designed as components of the PROCRUSTES testbed, linked and actuated through the **Scenario Planner**, an **evaluation toolkit** and an enhanced **cyber-physical stress-testing platform**, to model water distribution networks as CPS.

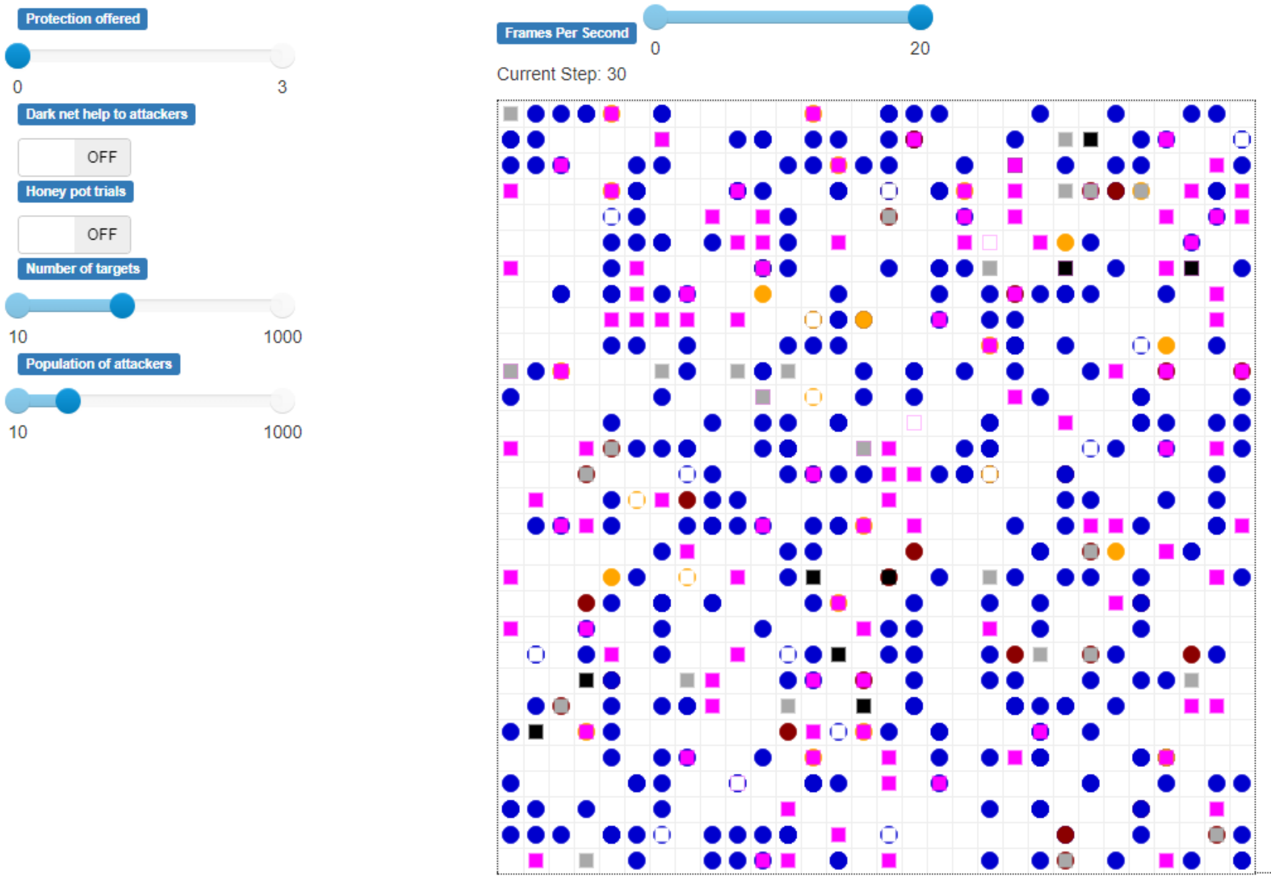
The PROCRUSTES testbed is designed to analyse and evaluate risks under uncertainty and stress-test mitigation options
(essentially a modern '*Procrustes bed*' for water systems)

CPRISK ABM [1/2]

Agent-based models render real-world socio-technical systems with dynamic interactions governed by independent **goal-driven behaviours**.

CPRISK ABM is a **generic approach**, adaptable to different CPS architecture, that explores the behaviour of CP attackers and their interaction with the critical cyber nodes of water CIs.

- Considers factors of **capability**, **motivation** and **opportunity** for the independent threat agents (Attackers) according to the security and **risk attitude** of a utility.
- Different "**protection levels**" according to the utility practices and applied measures.
- Distributed **honeypot networks** can gather valuable threat intelligence and protect CPS against adversary's techniques
- Access to **Darknet** provides advanced tools and techniques for threat actors to compromise assets/systems beyond their actual know-how / skills.



Protection offered
0 3

Dark net help to attackers
OFF

Honey pot trials
OFF

Number of targets
10 1000

Population of attackers
10 1000

Frames Per Second
0 20

Current Step: 30

Early prototype of CPRISK interface

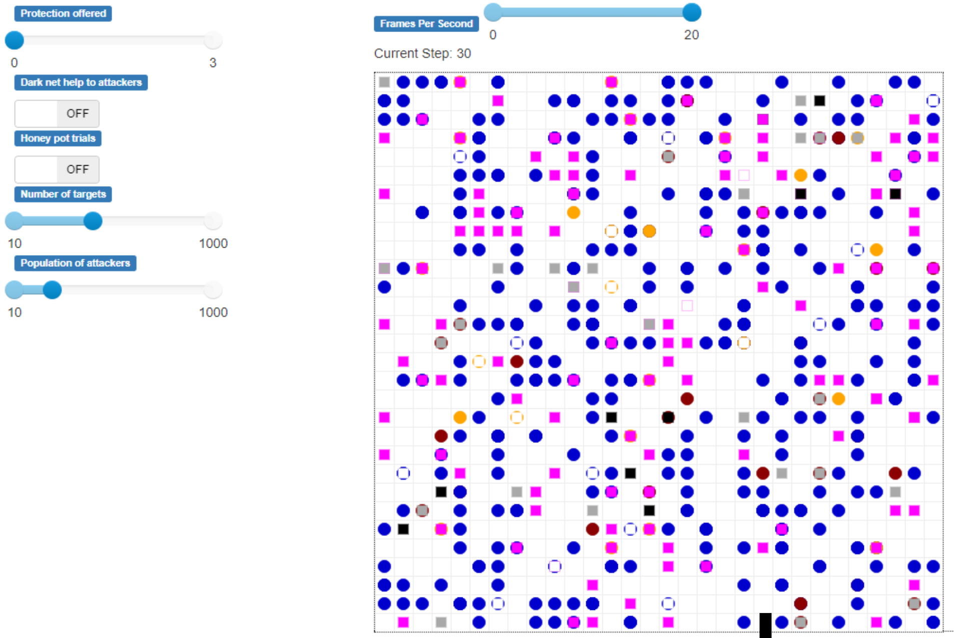
Blue circles depicts working Targets, **orange** depicts compromised Targets, **red** depicts Destroyed Targets, **magenda** squares depicts amateur Attackers, **grey** depicts expert Attackers and **black** depicts highly-skilled Attackers

CPRISK ABM [2/2]

Different security practices, or the occurrence of “attractive” events etc. instantly alter the dynamics of the threat landscape under examination…

Early **CPRISK ABM** results **capture** the trends and attacker type characteristics of **recorded** breaches **databases** and reports [18], as presented recently in [20].

Due to **sensitive nature** [19], **“frequency”** data are post-processed and introduced in a semi-quantitative form to the PROCRUSTES testbed.



Protection offered 0 3

Dark net help to attackers OFF

Honey pot trials OFF

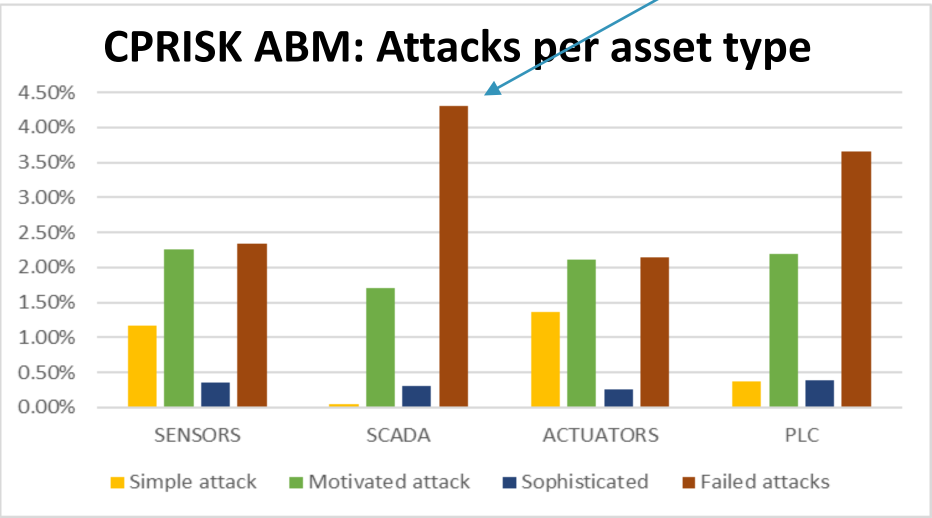
Number of targets 10 1000

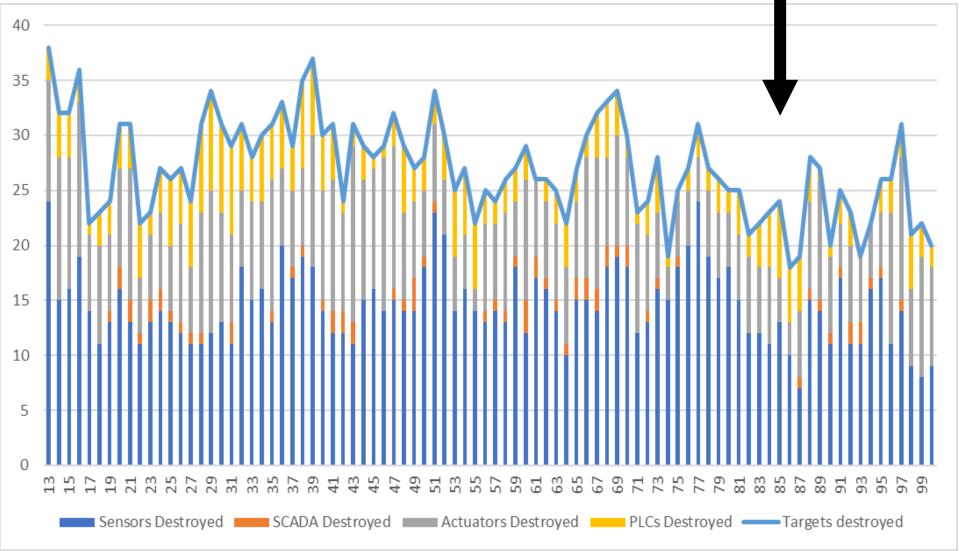
Population of attackers 10 1000

Frames Per Second 0 20

Current Step: 30

Higher protection of some asset types yields lower successful attacks…

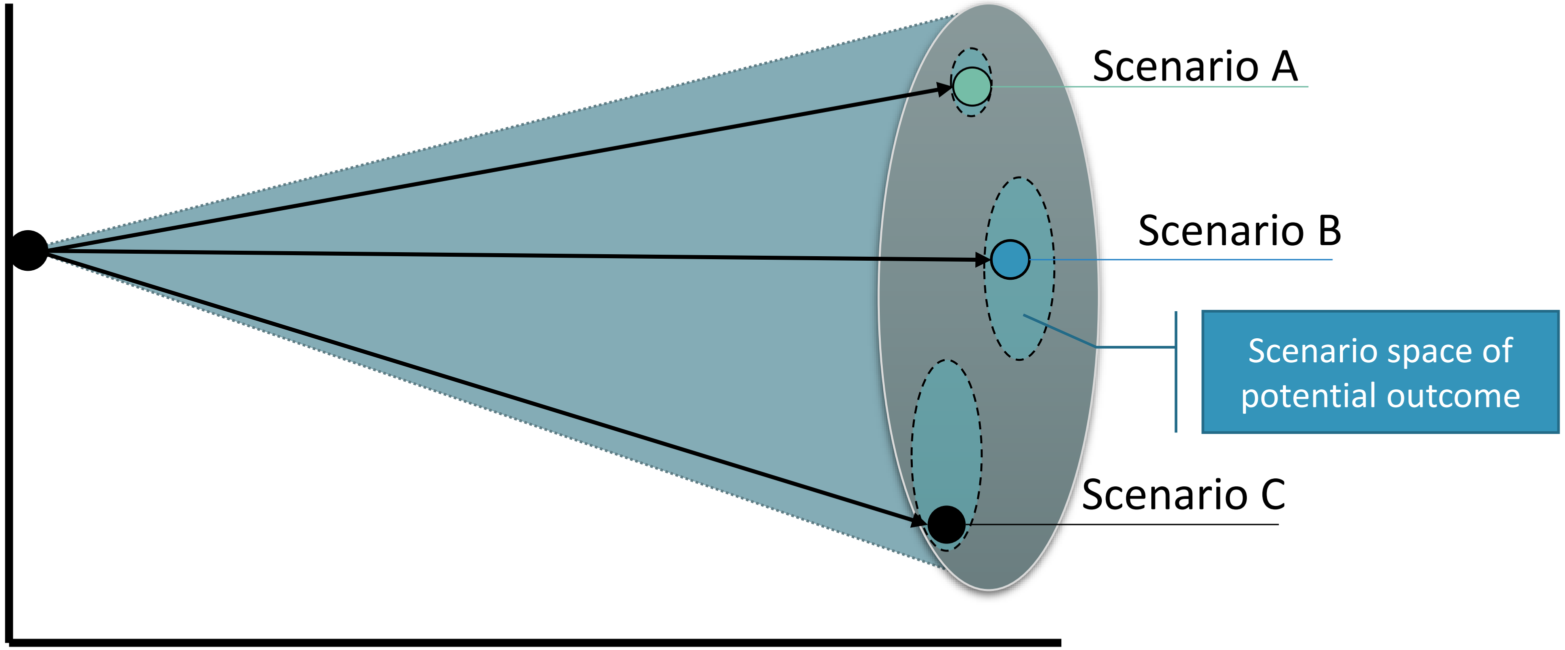




Optimisation Platform

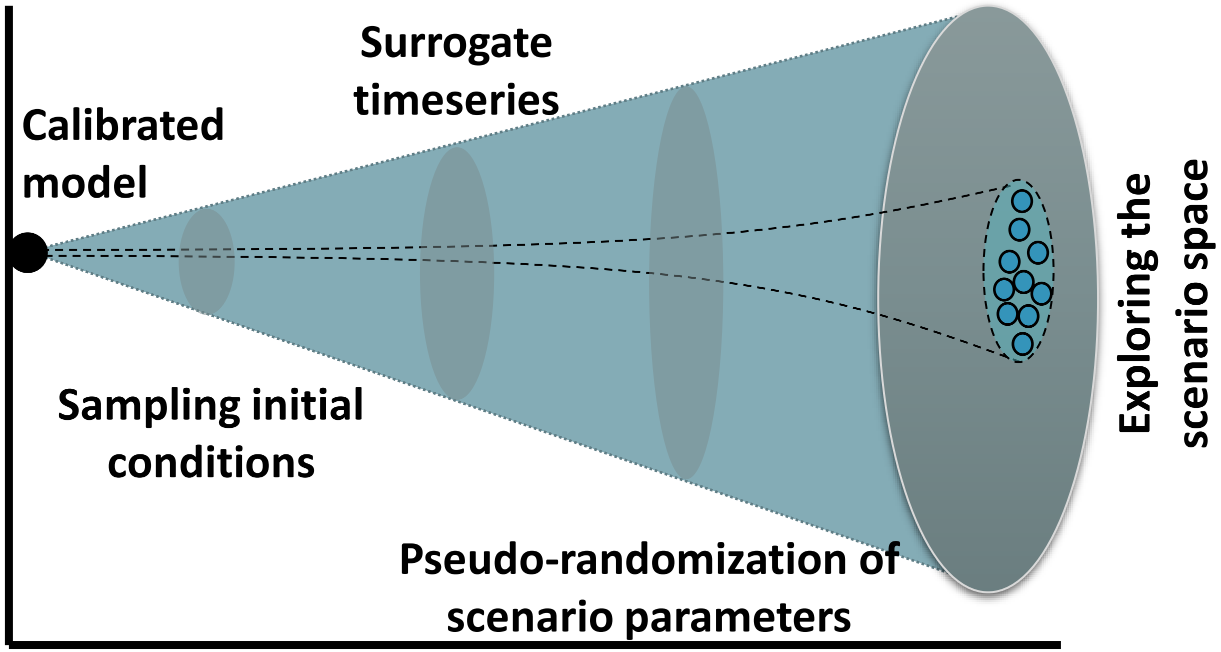
The **Optimisation Platform** will build, through embedded **multi-objective algorithms**, an automated process of **surrogate stochastic datasets** for water distribution models and support uncertainty-aware processes for the water CPS [21]. The process is designed to allow for:

- **Multi-objective algorithms** can help calibrate the models against multiple timeseries (historic or synthetic)
- Monte-Carlo, Orthogonal or Latin hypercube sampling (LHS) for **initial conditions** of the simulation models (e.g. tanks or reservoirs' initial storage, low concentration of disinfection at the WTP outflow etc.)



- Surrogate timeseries to explore the CPS behaviour under **stochastic boundary conditions**, utilizing advanced multivariant algorithms e.g. [22] for stochastic processes at single and **multiple temporal scales.** (e.g. synthetic demand timeseries)
- Platform **guided pseudo-randomisation** of threat **scenario parameters** to help identify most **critical components** (against different evaluation metrics) for an ABM-derived combination of threats

Scenario Planning


Surrogate timeseries
Calibrated model
Sampling initial conditions
Pseudo-randomization of scenario parameters
Exploring the scenario space

Scenario Planner's advanced filters applied through a looped process with the Optimisation Platform, broadens the scenario horizon

The **Scenario Planner (SP)** enables the ***what-if* investigation** of threat events or more complex combination of them.

- The basic layout supports **user-defined**, **single scenario** formulation to explore specific conditions

- SP can utilise the CPRISK ABM derived attack frequency data to propose and **synthesise** scenarios of **"most probable"** threats against the system

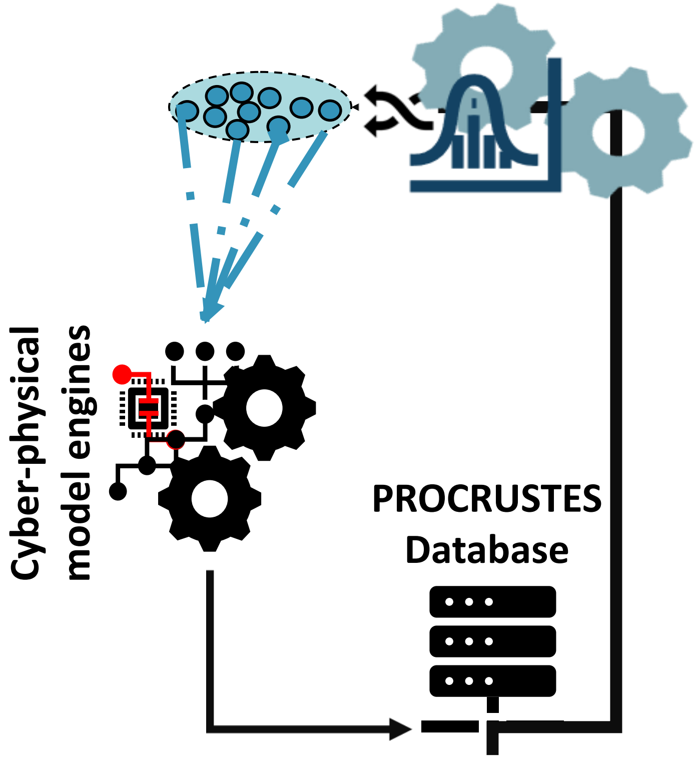
- At the advanced level, **SP** supports novel, **automated** capabilities through the **looped interaction** with the **Optimisation Platform** to organize risk analysis under uncertainty though sampling techniques, surrogate timeseries and pseudorandomisation of parameters (e.g. asset attacked, start-time etc.).

- At all levels, the tool **"links" the threats to the network-specific assets**, utilising a threat taxonomy and a network segregator which identifies and lists the assets from the network model. This also allows it to act as a **model aggregator** and synthesize the **model-appropriate files** for the stress-testing **simulation**.

Models for stress-testing

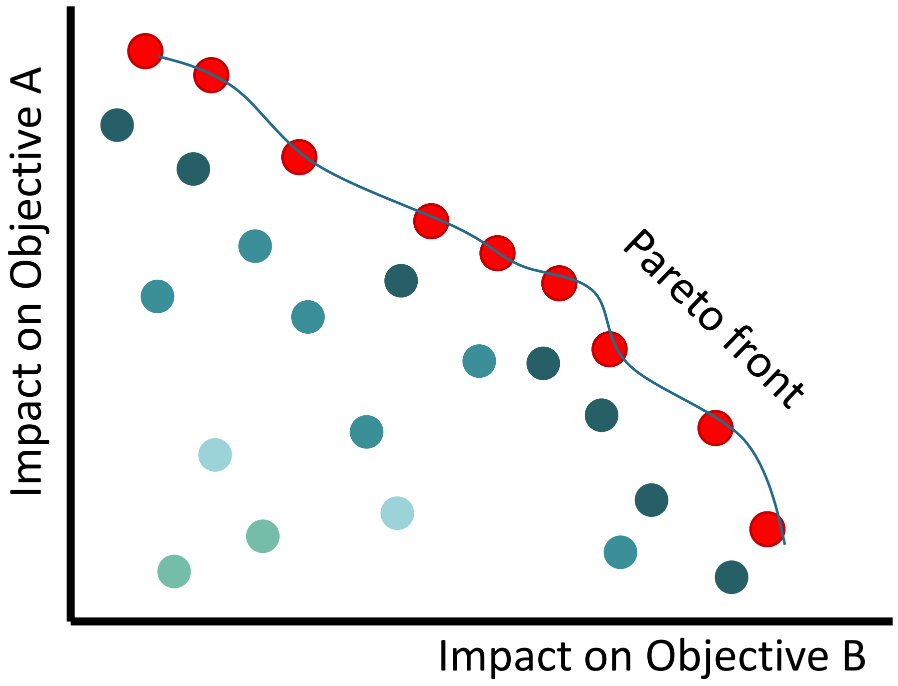
The PROCRUSTES Stress-testing Platform advances existing approaches and follows the **Scenario Planner** and **Optimisation Platform processes** to configure the probabilistic scenario set-up and **assess** CPS **considering stochastic boundary conditions**.

- The PROCRUSTES embedded engines will support multiscale modelling for the water system for both **hydraulic modelling** and **contamination events** propagation in water distribution networks.
- Based on modified EPANET engines such as RISKNOUGHT [23], able to perform Demand Driven and **Pressure Driven Analysis (for realistic modelling of systems under stress)**, while coupling the hydraulic operations with the cyber model of the control logic.
- Seeking surrogate or parallel computing architecture transformation of the Stress-testing Platform to deal with the computationally-demanding and time-consuming process.
- Simulate scenarios guided by the Optimisation Platform filters and Scenario Planner capabilities, to **encapsulate the uncertainty** of a potential threat' success on specific assets and provide an assessment of **the overall risk evolution**.



Evaluating and prioritizing threats

Evaluation and prioritization of representative consequences space



Data form the stress-testing platform are accessible for the **Evaluation and Prioritization toolkit**, through the PROCRUSTES Scenario Database. The toolkit will include a variety of objective performance indicators to measure the loss of performance for the water CPS.

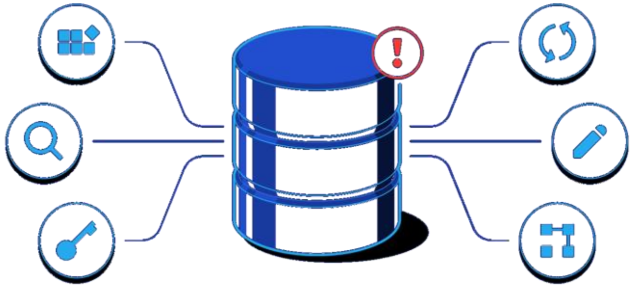
- Performance indicators used render the different threat outcome characteristics in terms of **operational** and **societal impact at different spatial level**, while considering **critical customers** (e.g. hospitals) (based on [24]) and provide valuable information for both risk assessors and first responders.

- **Normalised** indicators' values allow the **comparison** of corresponding **under the probabilistic approach** and stochastic boundary conditions – which alter the steady reference to a single common business-as-usual scenario.

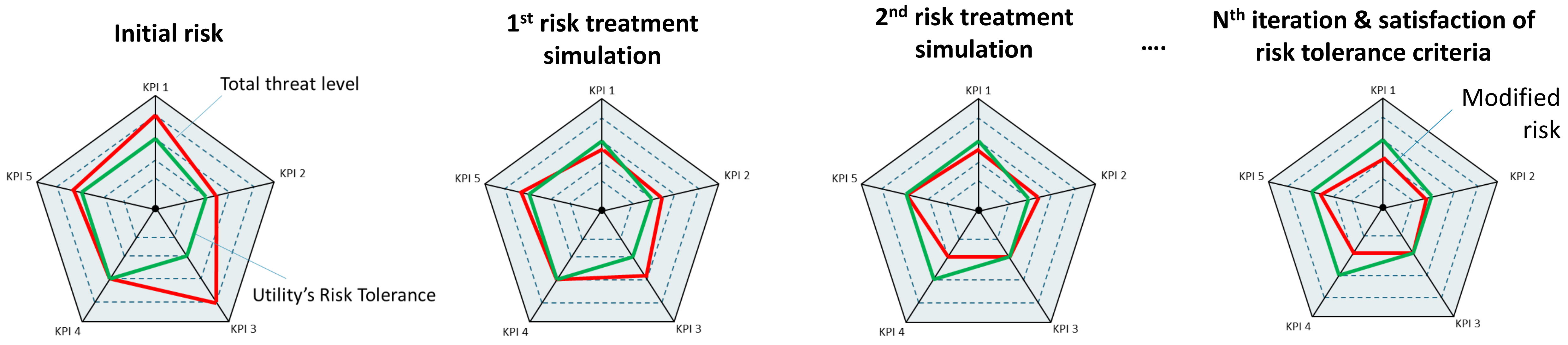
- Utilizing the **Optimisation Platform** capabilities and user defined **risk criteria**, the toolkit will be able to **prioritise** (rank) **risks** to be treated and **indicate critical assets** against different metrics (e.g. Unmet Demand %, Customer Minutes Lost, Detection time of chemical contamination, system survival time etc.)

Stress-testing the treatment options

The dynamic Risk Reduction Knowledge-Base (**RRKB**) will contain actions, activities or processes to reduce the level of risk either by **modifying the likelihood and/or** by changing the **consequences.**



- **RRKB's taxonomy** to uniquely map measures for each risk
- Dynamic user interface and filtering/shorting capabilities
- Expandable structure to allow integration of new state-of-art measures and best-practices
- **Linked** to the **Stress-testing Platform**, to assess the measures performance through the looped process of stress-testing and modify risks **to meet risk tolerance criteria** (optimum level)



Initial risk

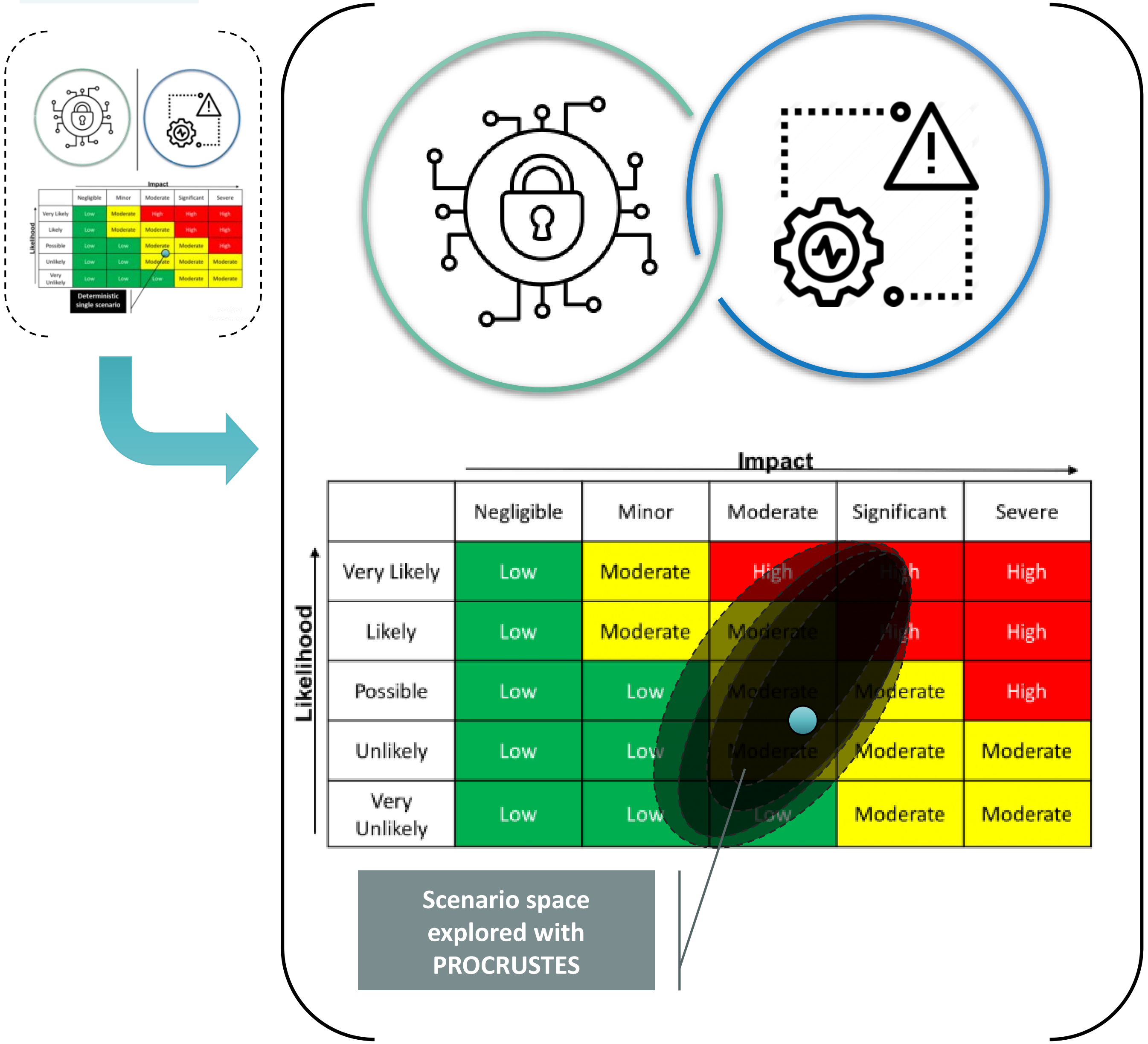
1st risk treatment simulation

2nd risk treatment simulation

....

Nth iteration & satisfaction of risk tolerance criteria

Conclusion[1/2]



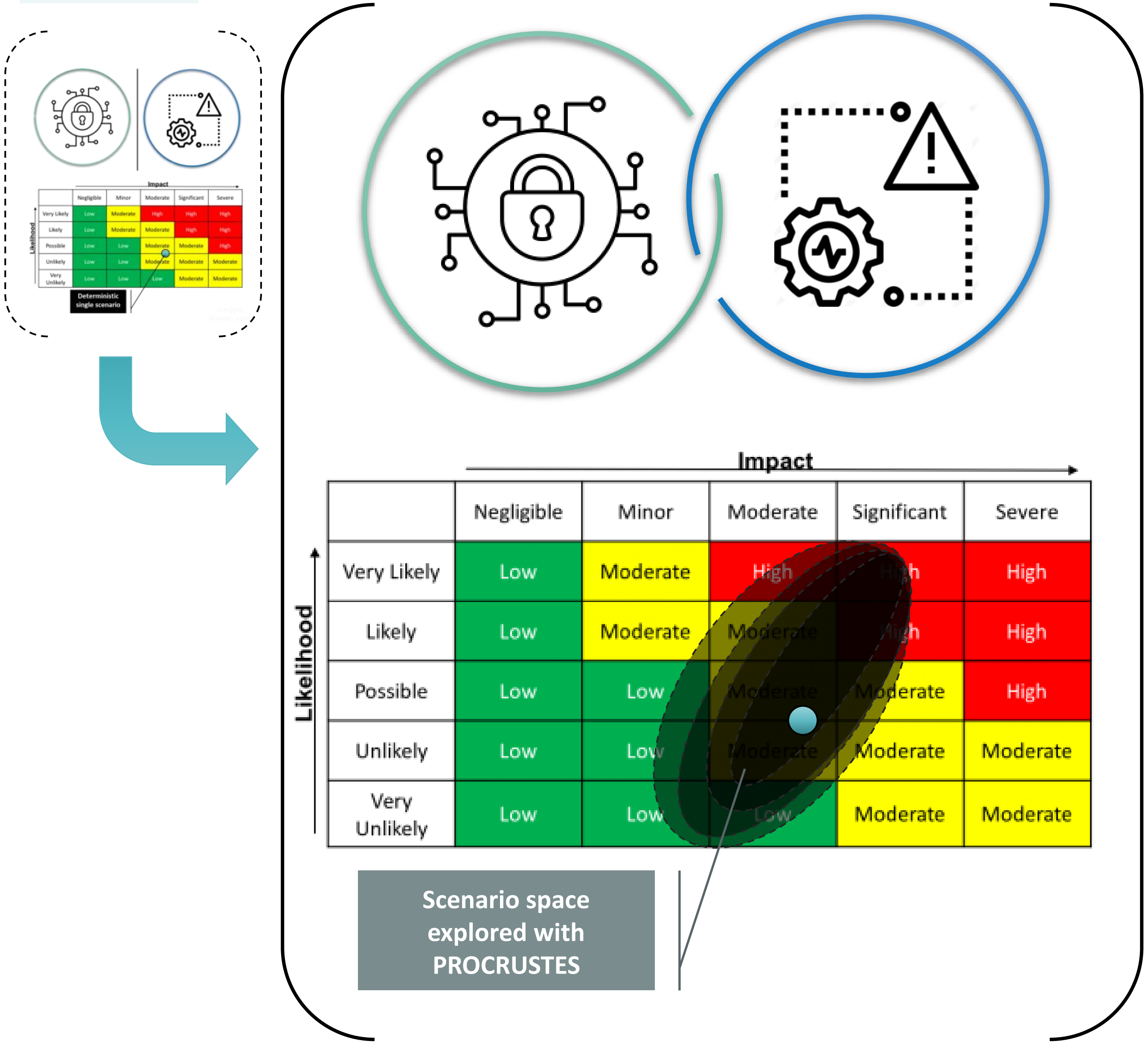
	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

Scenario space explored with PROCRUSTES

PROCRUSTES project will bring forth a risk assessment framework and associated toolkit able to **analyse** and **evaluate** physical and cyber **risks** on water critical infrastructures (CIs) and their combinations as well as to support the choice of appropriate **risk treatment** options and evaluate their effectiveness under **uncertainty**.

- The generic CPRISK ABM approach can model the goal-driven behavioural rules of adversaries against key cyber assets of CPS and derive actionable attack likelihood data.
- The Optimsation Platform and relevant probabilistic approach to examine the scenario space, prioritise risks and promote an uncertainty-aware decision making process against emerging threats

Conclusion[2/2]



	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

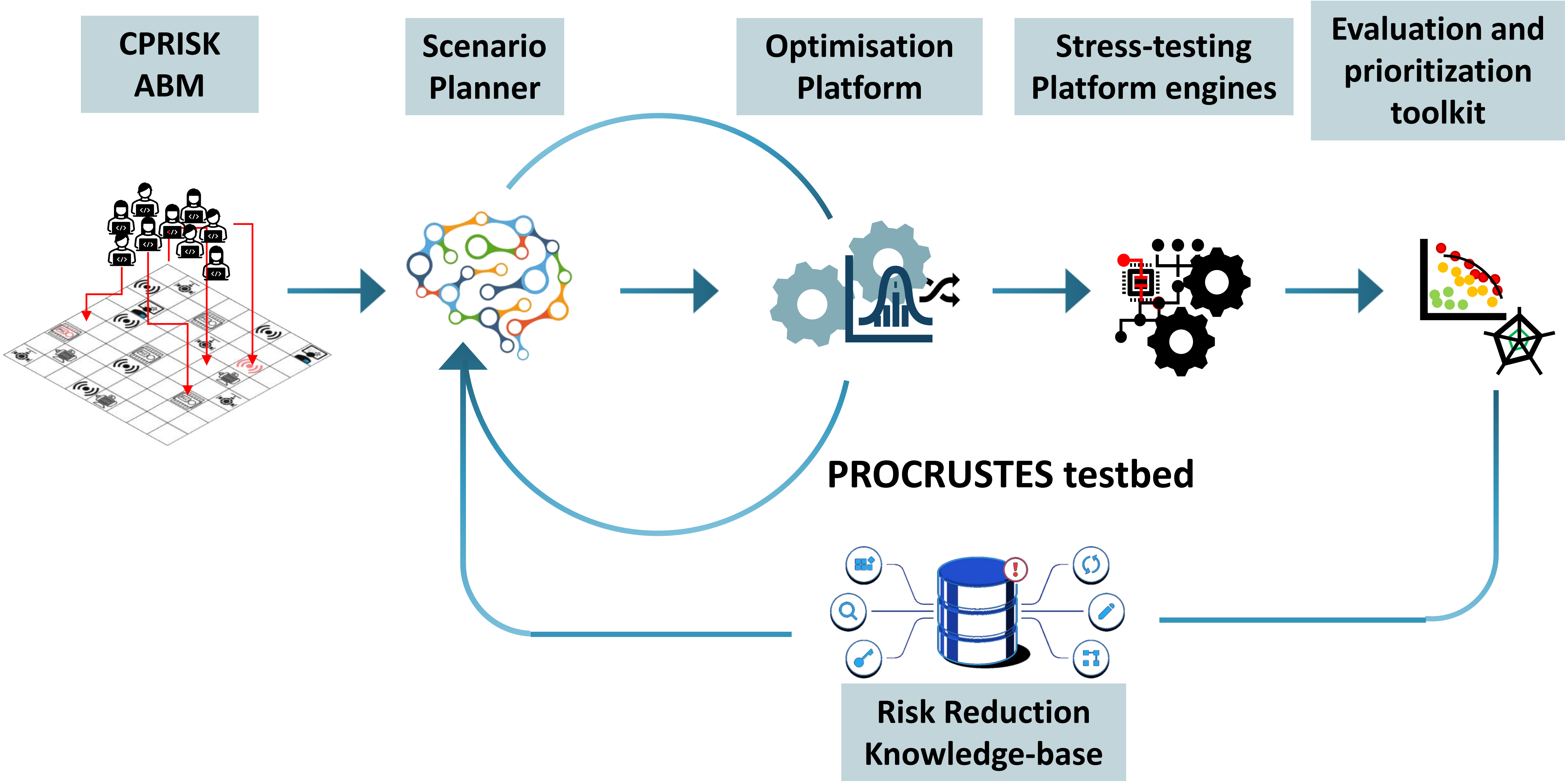
Scenario space explored with PROCRUSTES

- Enhanced Scenario Planning capabilities can automatically formulate different scenario set-ups (e.g. most probable attack) and incorporate into model-specific files the outputs of the Optimisation Platform

- A Stress-testing platform will simulate the combined physical and logical (cyber) layers of a network and assess the effects of a threat, under stochastic boundary conditions, in both hydraulic and quality dimensions.

- The comprehensive, expandable RRKB will be able to recommend suitable actions for to modify the risk events' likelihood or consequences, altering the risk level to fit within a utility's risk tolerance limits and enhance its resilience.

The PROCRUSTES testbed



CPRISK ABM

Scenario Planner

Optimisation Platform

Stress-testing Platform engines

Evaluation and prioritization toolkit

PROCRUSTES testbed

Risk Reduction Knowledge-base

References

[1] Rasekh A., Hassanzadeh A., Mulchandani S., Modi S., Banks M.K. (2016) Smart water networks and cyber security. Journal of Water Resources Planning and Management 142(7): 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646

[2] Jill, J.S.; Miller, M. (2008). Lessons Learned from the MaroochyWater Breach. Critical Infrastructure Protection; Springer: New York, NY, USA; Vol. 253, 73–82.

[3] Hassanzadeh, A., A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, and M. K. Banks. 2020. "A review of cybersecurity incidents in the water sector." J. Environ. Eng. 146 (5): 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686

[4] U.S. Department of Homeland Security (DHS), US-CERT, Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, March 15, 2018, revised, March 16, 2018, https://www.us-cert. gov/ncas/alerts/TA18-074A; U.S. DHS, US-CERT, Alert (TA18-106A), Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, April 16, 2018, revised, April 20, 2018, https://www.us-cert.gov/ncas/alerts/TA18-106A

[5] The United States Department of Justice. United States District Court Southern District of New York: Sealed Indictment. (2016). https://www.justice.gov/opa/file/834996/download

[6] Janke, R., M. E. Tryby, and R. M. Clark. "Protecting water supply critical infrastructure: An overview." Securing Water and Wastewater Systems. Springer International Publishing, 2014. 29-85.

[7] Zhu, B., A. Joseph, and S. Sastry. "A taxonomy of cyber-attacks on SCADA systems." Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing. IEEE, 2011.

[8] Nikolopoulos, D., G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, and C. Makropoulos (2020) "Cyber-physical stress-testing platform for water distribution networks." J. Environ. Eng. 146 (7): 04020061. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001722

[9] N. Pelekanos, D. Nikolopoulos & C. Makropoulos (2021) Simulation and vulnerability assessment of water distribution networks under deliberate contamination attacks, Urban Water Journal, 18:4, 209-222, https://doi.org/10.1080/1573062X.2020.1864832

[10] Culp, S., Thompson, C., 2016. The Convergence of Operational Risk and Cyber Security. Chartis.

[11] Makropoulos, C., Savíc, D.A., 2019. Urban hydroinformatics: Past, present and future. Water (Switzerland) 11. https://doi.org/10.3390/w11101959

References

[12] Wangen, G., 2019. Quantifying and Analyzing Information Security Risk from Incident Data. pp. 129–154. https://doi.org/10.1007/978-3-030-36537-0_7

[13] Florêncio, D., Herley, C., 2013. Sex, Lies and Cyber-Crime Surveys, in: Schneier, B. (Ed.), Economics of Information Security and Privacy III. Springer New York, New York, NY, pp. 35–53. https://doi.org/10.1007/978-1-4614-1981-5_3

[14] Loukas, G. 2015. "Cyber-physical attacks on industrial control systems." In Cyber-physical attacks, 105–144. Amsterdam, Netherlands: Elsevier.

[15] H. Wheater, K. Beven, J. Hall, G. Pender, D. Butler, A. Calver, S. Djordjevic, E. Evans, Makropoulos, C., E. O'Connell, E. Penning-Rowsell, A. Saul, S. Surendran, I. Townend, A. Watkinson, "Broad Scale Modelling for Planning and Policy", R&D Technical Report FD2118, Joint Defra/EA Flood and Coastal Erosion Risk Management R&D Programme

[16] Filatova, T., P.H. Verburg, D.C. Parker, C.A. Stannard, "Spatial agent-based models for socio-ecological systems: challenges and prospects", Environmental Modelling & Software, 45 (2013), pp. 1-7

[17] Koutiva, I., and C., Makropoulos. (2016). "Modelling domestic water demand: An agent based approach.“ Environmental Modelling & Software 79:35-54.

[18] Verizon, 2017. 2017 Data Breach Investigations Report Tips on Getting the Most from This Report. Verizon Bus. J. 1–48. https://doi.org/10.1017/CBO9781107415324.004

[19] NIST, 2012. Guide for conducting risk assessments. NIST Spec. Publ. 95. https://doi.org/10.6028/NIST.SP.800-30r1

[20] Koutiva I., Moraitis G, Makropoulos C. (2021 - under review) . An Agent-Based Modelling approach to assess risk in Cyber-Physical Systems (CPS). 17th International Conference on Environmental Science and Technology - CEST 2021, 1-7 September, Athens

[21] P. Kossieris, I. Tsoukalas, C. Makropoulos, and D. Savic. (2019) Simulating marginal and dependence behaviour of water demand processes at any fine time scale, Water, 11 (5), 885, https://doi.org/10.3390/w11050885

[22] I. Tsoukalas, P. Kossieris, and C. Makropoulos. (2020) Simulation of non-Gaussian correlated random variables, stochastic processes and random fields: Introducing the anySim R-Package for environmental applications and beyond, Water, 12 (6), 1645, https://doi.org/10.3390/w12061645

[23] Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C., 2020. RISKNOUGHT: Stress-testing platform for cyber-physical water distribution networks HS5.2.3-Water resources policy and management: digital water and interconnected urban infrastructure. https://doi.org/10.5194/egusphere-egu2020-19647

[24] Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C., 2020. Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. J. Environ. Eng. 146, 04020108. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001765

Acknowledgement

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded 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)

Principal Investigator: Prof. Christos Makropoulos

cmakro@mail.ntua.gr

PROCRUSTES

http://www.procrustes.gr/en/

The PROCRUSTES testbed:

tackling cyber-physical risk for water systems

Georgios Moraitis*, Dionysios Nikolopoulos, Ifigeneia Koutiva, Ioannis Tsoukalas, George Karavokiros, and Christos Makropoulos

EGU21-14903, EGU General Assembly 2021
https://doi.org/10.5194/egusphere-egu21-14903

[Session HS5.4.1]

***corresponding author: Georgios Moraitis**
georgemoraitis@mail.ntua.gr

School of Civil Engineering
National Tech. Univ. of Athens

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded 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)