Iceland
Liechtenstein
Norway grants

"Working together for a green, competitive and inclusive Europe"

Project: *Digitalisation of water sector and water education* - **DIGIWATRO**,
Contract: 20-COP-0050

Intellectual Output 1: *Enhancing Digital Surveillance, Automation and Cybersecurity in Water Utilities Boosting*

Disclaimer

This document was realized with the EEA Financial Mechanism 2014-2021 financial support. Its content (text, photos, videos) does not reflect the official opinion of the Programme Operator, the National Contact Point and the Financial Mechanism Office. Responsibility for the information and views expressed therein lies entirely with the authors.

UNIVERSITAS GALATIENSIS

Norwegian University of Life Sciences

Introduction

The first Intellectual Output of the DigiwatRO project had as objective to develop, test, and validate illustrative concepts for digital surveillance, automation, and cybersecurity in the water sector.

The impact of the obtained results was observed at three levels: scientific, academic, and industrial.

(1) from a scientific point of view the impact can be observed through the papers that resulted from the current project. The research undertaken in this project already forms the basis for related research. In addition, the analysis methods developed in this project will be used in future research in the digitalization of the water sector.
(2) at the academic level, the impact of the project results places the research teams in the landscape of digitization of the water sector. Each member of the team has gained experience in this highly promising field, an impact that will be seen in the long term. This is one of the most significant results as the teams will be able to propose new international projects in the field of digitization of the water sector. The expertise of the teams can be demonstrated by the results disseminated from this project.
(3) At industry level, the teams' expertise is used to transfer technology to the private sector. The workshop organized at ETFA 2023 in this project involved the presence of companies from the automation sector.

Water sector and especially the water utilities are undergoing a rapid digitalization leading to new investments, new equipment, generating a huge amount of online data, increased remote monitoring and control. The information generated by this project are grossly underutilized for process control. Thus, one aspect is to explore and develop concepts to improve the data quality and their use for better process m0onitoring. Another great danger which the water utilities are facing is the risk of cyber threats. The most water utilities are not aware of these dangers and objective is to increase the awareness, preparedness, and the rapid recovery in case of an event.

Within the issues generated by the water sector, three main scientific areas have been identified and investigated in this project:

- Process Monitoring and Control Systems
- Virtual Sensors
- Analysis of the Cybersecurity Incidents in the Water Sector

In establishing these areas, the structure and equipment of the treatment plants in Romania (Galați) and Norway (Oslo) were considered. Three papers resulted from investigating these scientific areas and were presented at the 28th International Conference on Emerging Technologies and Factory Automation – ETFA 2023, Sinaia, Romania, sept. 12 – 15 (https://2023.ieee-etfa.org/main/static/files/program/ConferenceProgram_Complete.pdf):

- Ratnaweera H, Nair A, Hykkerud A, Sivchenko N, Ratnaweera D, Condrachi L. Achieving legislative requirements in wastewater treatment using digital tools. ETFA 2023
- Ghinea LM, Miron M, Ratnaweera H. A Deep Learning Approach for Faults Recognition of Dissolved Oxygen Sensor in Wastewater Treatment Plants. ETFA 2023
- Țîru AE, Vasiliev I, Diaconu L, Vilanova R, Voipan D, Ratnaweera H. Integration of ANN for Accurate Estimation and Control in Wastewater Treatment. ETFA 2023

1. Process Monitoring and Control Systems

Fault diagnosis in wastewater treatment plants (WWTPs) is important to protect communities and ecosystems from toxic elements discharged into water. In this sense, fault identification of sensors plays an important role as they are the key components of the water plants control, especially because environmental legislation is very strict when referring to failures or anomalies in WWTPs.

1.1.A Deep Learning Approach for Faults Recognition of Dissolved Oxygen Sensor in Wastewater Treatment Plants

This case study evaluates the performances of two deep learning algorithms (FFNN - Feedforward Neural Network and 1DCNN - Convolutional Neural Network) for identifying 4 different mechanical faults which can occur in DO sensor of a Wastewater Treatment Process (WWTP). All the faults were analyzed via Benchmark Simulation Model no 2, developed by the IWA Task Group (Alex at al., 2008). The structure of the plant is identical to that of the wastewater treatment plant in Galati city. For this purpose, were implemented fault blocks in Matlab Simulink 2022a and developed two neural classifiers in Google Colaboratory (Colab) environment with the Python open-source libraries: Scikit-Learn 1.2.2 and TensorFlow 2.12 with Keras, a high- level Deep Learning API integrated.

In this study are analyzed the following faults scenarios:

1. Bias fault – occurs due to a constant offset (v) in the sensor output measurements. Bias fault injection can be implemented by adding a constant value to the sensor output. As a result, a shift from the normal value is produced on the DO output, mathematically defined:

$$s(t) = h(t) + \eta + u, u = constant \qquad (1.1)$$

   where $s(t) = h(t) + \eta$ is the expected output of the sensor without the presence of faults, $h(t)$ is the output of the sensor at time t and η is the noise.

2. Stuck fault - occurs when a sensor becomes "stuck" in a particular state or position, failing to respond to changes of the system. Stuck fault injection means that the sensor output is locked at a fixed value v for a temporary or permanent period. As a result, a complete failure is produced on the DO output, mathematically defined:

$$s(t) = u, u = constant \qquad (1.2)$$

3. Spike fault – when large amplitude peaks occur at the DO sensor output. The spike fault injection is performed, as the name indicates, by large amplitude peaks at constant time intervals (r). To mathematically define a spike fault, a constant bias b_t is added to the elements of the normal signal, as below:

$$s(t) = h(t) + \eta + b_t \quad (1.3)$$
$$\forall\, t \in u \times r$$

where $v = \{1, 2, \ldots\}$ is a set of natural numbers and r is the interval in which the spikes occur in the sensor output, with $r \geq 2$.

4. Precision degradation (PD) – occurs as a loss of precision in the sensors or control systems used to monitor and control the treatment process. PD fault injection is performed by adding a noise with zero mean and high variance to the output of DO sensor, mathematically defined:

$$s(t) = h(t) + \eta + v \sim N(0, \delta_v^2), \delta_v^2 \gg \delta_n^2 \quad (1.4)$$

where δ_v^2 is the noise with zero mean and high variance.

Table 1.1 shows the duration and the start day of each fault scenario that was analyzed.

Table 1.1 Faults of DO sensor signal

Fault	**Start [day]**	**Duration [hours]**
Bias	280	480
Stuck	350	600
Spike	400, 420, 440, 460	48
PD	500	720

According to (Alex at al., 2008), the plant model is simulated during a period of 609 days. Data is evaluated at each 15 minutes interval starting from 245th day. The following faults scenarios (Fig. 2.1-2.4) were analyzed in our study: bias, stuck, spike and precision degradation (PD).

The bias fault scenario from Fig. 1.1 is generated in the DO sensor, during a period of 20 days. This type of fault is characterized by a constant difference between the true value and the faulty DO sensor output of +1.5 mg/L (Liu et al., 2022).

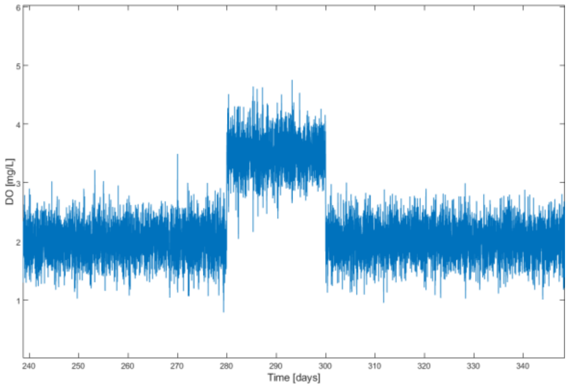


Fig. 1.1. Bias fault of DO sensor

The stuck fault scenario from Fig. 1.2 is induced in the DO sensor during a period of 25 days. This type of fault indicates that the DO sensor measurements freeze at a fixed value, in this case scenario at 2 mg/L and is not responding anymore to any variation of DO concentration. This fault is considered a complete failure which could be a temporary or permanent issue.

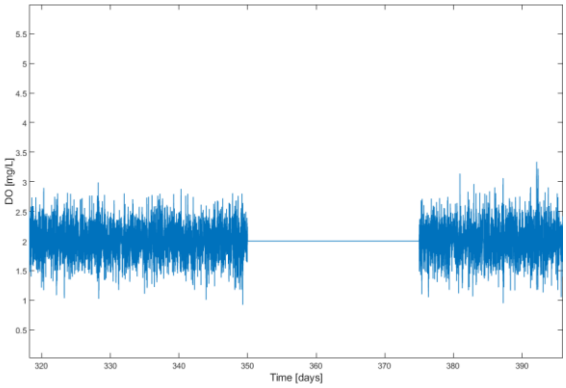


Fig. 1.2. Stuck fault of DO sensor

The spike fault scenario from Fig. 1.3 is generated in the DO sensor output during 4 – time intervals with different amplitude, consisting of 2 days each.

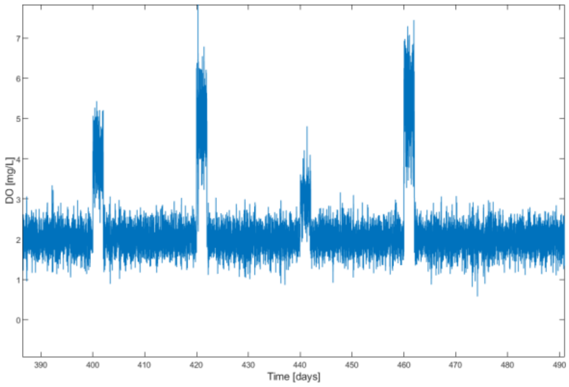


Fig. 1.3. Spike fault of DO sensor

The precision degradation (PD) fault scenario from Fig. 1.4 is implemented in the DO sensor, over a period of 30 days. This type of fault consists of adding a noise with zero mean and high variance to the sensor output.

Deep learning techniques are intensively used in the field of fault diagnosis in WWTPs. Moreover, these processes are complex, dynamic, and nonlinear, often prone to failures, uncertainties, and disturbances. From this perspective, it’s important to have performant tools such as Neural Networks (NNs) to identify with high precision and efficiency any mechanical faults which can occur in these processes, especially in case of sensors used to control energy consumption and discharge quality (Chi and Guo, 2019; Mamandipoor et al., 2020).

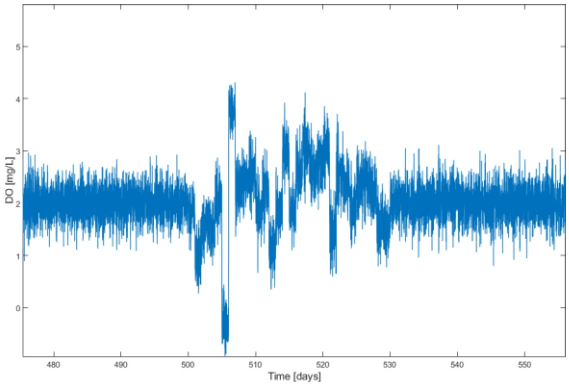


Fig. 1.4. Precision degradation (PD) fault of DO sensor

For example, in the case of dissolved oxygen sensors, the aeration systems depend on the values measured by the DO sensor, so any failure in this signal can affect the system normal operation (Salles et al., 2023).

In this sense, the current study compares two neural models, FFNN vs. 1DCNN. The purpose is to establish which DL classifier is capable of accurately identifying the 5 operating states of DO sensor faults in WWTP: normal (class 0), bias (class 1), stuck (class 2), spike (class 3) and precision degradation (PD) (class 4).

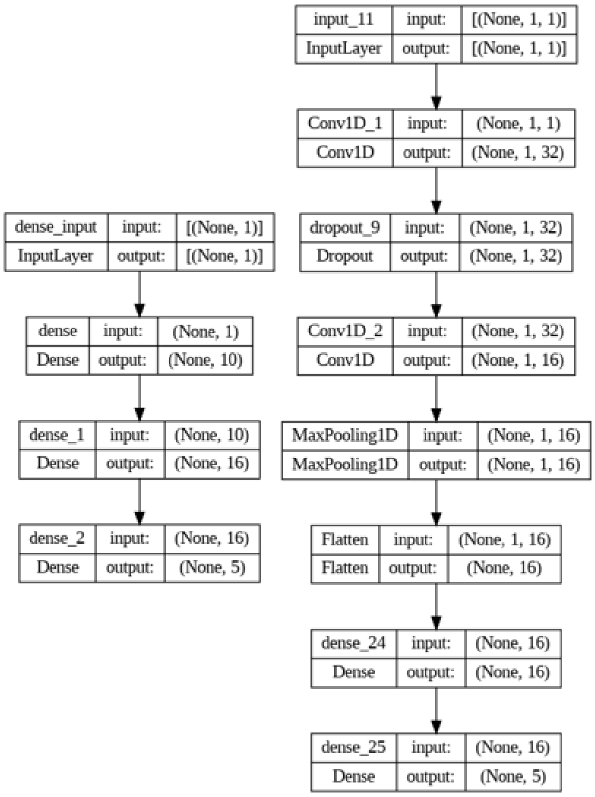

dense_input | input: | [(None, 1)]
InputLayer | output: | [(None, 1)]
dense | input: | (None, 1)
Dense | output: | (None, 10)
dense_1 | input: | (None, 10)
Dense | output: | (None, 16)
dense_2 | input: | (None, 16)
Dense | output: | (None, 5)
input_11 | input: | [(None, 1, 1)]
InputLayer | output: | [(None, 1, 1)]
Conv1D_1 | input: | (None, 1, 1)
Conv1D | output: | (None, 1, 32)
dropout_9 | input: | (None, 1, 32)
Dropout | output: | (None, 1, 32)
Conv1D_2 | input: | (None, 1, 32)
Conv1D | output: | (None, 1, 16)
MaxPooling1D | input: | (None, 1, 16)
MaxPooling1D | output: | (None, 1, 16)
Flatten | input: | (None, 1, 16)
Flatten | output: | (None, 16)
dense_24 | input: | (None, 16)
Dense | output: | (None, 16)
dense_25 | input: | (None, 16)
Dense | output: | (None, 5)

Fig. 1.5. Deep Learning architectures: a) FFNN and b) 1DCNN

The architecture of each DL is presented in Fig. 1.5. In the case of FFNN, the layers are added sequentially: input layer (10 neurons, ReLU - activation function), 1 hidden layer (16 neurons and ReLU - activation function) and output layer (5 neurons and Softmax - activation function). To overcome overfitting, the activity regularization is set to 0.01 in the input layer of the neural model. However, in the case of 1DCNN, the layers are: Conv1D layer (filters=32, kernel_size=1, activation='relu'), Dropout layer (dropout rate=0.2), Conv1D layer (filters=16, kernel_size=1, activation='relu'), MaxPool1D layer (pool_size=1), Flatten layer, Dense layer (16 neurons, activation='relu') and Dense layer (5 neurons, activation='softmax').

Both DLs are compiled with Categorical Cross Entropy Loss function, Adam optimizer (learning rate=0.001) and Accuracy metric for evaluating the model during training and validation. Also, the training is performed with the fit() method from Keras API and iterated over 100 epochs. From the dataset are selected 80% for training and 20% for testing.

The hyperparameters of the neural networks were selected around the values suggested by the KerasTuner, a general purpose hyperparameter tuning library.

The performances metrics used to evaluate the neural model are:

- Accuracy

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{1.5}$$

where TP – true positive, TN – true negative, FP – false positive and FN – false negative, all obtained from the confusion matrix.

- Precision

$$Precision = \frac{TP}{TP+FP} \tag{1.6}$$

where Precision – represents the positive predicted data.

- Recall

$$Recall = \frac{TP}{TP+FN} \tag{1.7}$$

where *Recall* – calculates the percentage of all data identified in a relevant class.

- F1-score

$$F1 - score = 2\frac{Precision \cdot Recall}{Precision+Recall} = \frac{2TP}{2TP+FP+FN} \tag{1.8}$$

where F1-score – represents the harmonic mean of the model precision and recall.

The DLs obtained FFNN - 98.32% overall training accuracy and 98.30% overall testing accuracy and 1DCNN - 92.76% overall training accuracy and 92.90% overall testing accuracy. The confusion matrices of DLs are presented in Fig. 1.6. The confusion matrix of FFNN demonstrates that the model classifies correctly in a proportion of 98.3% (11494 data from a total of 11693) and erroneous in a proportion of 1.7% (199 data from a total of 11693). However, the confusion matrix of 1DCNN shows that the model classifies correctly in a proportion of 92.90% (10863 data from a total of 11693) and erroneous in a proportion of 7.1% (830 data from a total of 11693). Based on these results, it becomes obvious that FFNN outperforms 1DCNN. This was highlighted in the classification report from Figure 1.7, with a red dotted line.

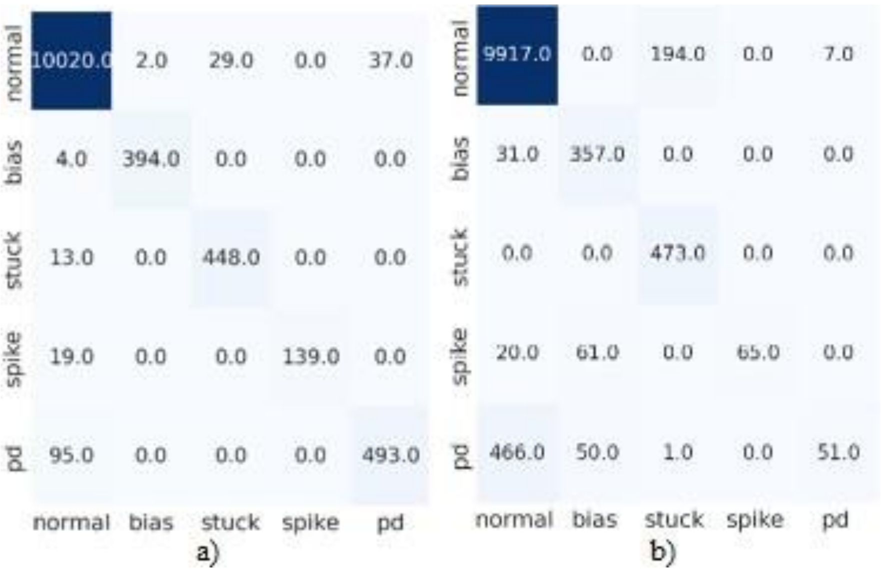


Fig. 1.6. Confusion matrices of DLs: a) FFNN and b) 1DCNN

According to Fig. 1.7, the best classification results are obtained in the case of Bias sensor fault with FFNN (99.49% Precision, 98.99% Recall and 99.24% F1-score) and the worst results are in the case of PD sensor fault with 1DCNN (87.93% precision, 0.08% recall and 0.16% F1-score). This indicates that PD support data from 1DCNN are imbalanced in comparison with the other classes. Thus, collecting more data might be required to improve the 1DCNN model performance. Nevertheless, our study reveals that FFNN has better performances and adaptability than 1DCNN and is a very powerful DL tool for enhancing DO sensor fault recognition in WWTPs.

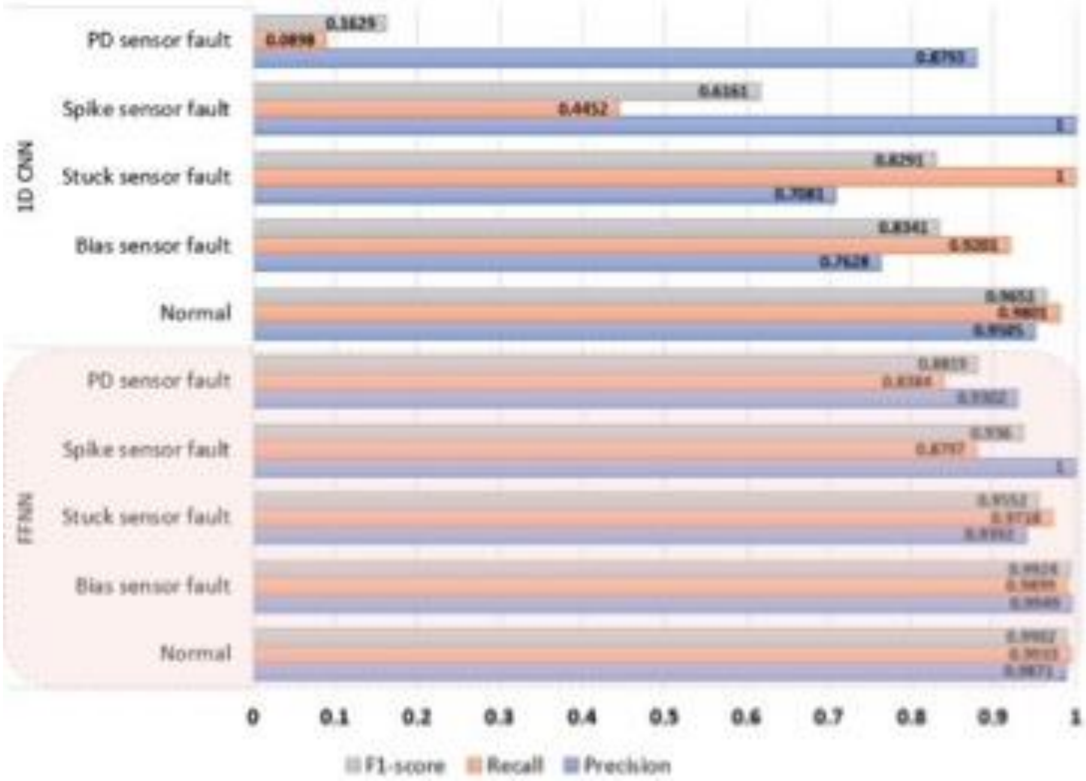


Fig. 1.7. Metrics (F1-score, Recall, Precision) of FFNN and 1DCNN

The FFNN is very efficient compared to 1DCNN for enhancing the fault recognition of the dissolved oxygen sensor.

1.2.Control of a wastewater treatment process using linear and nonlinear model predictive control

Control of the wastewater treatment process is not a trivial task, since the system is nonlinear, features large time con- stants and delays, and the interaction between variables is important (Luenberger, 1979). Thus, Model Predictive Control (MPC) framekwork is a good approach for such a demanding task, because of one important advantage: MPC has the ability to handle complex constraints and nonlinearities, which are typical of wastewater treatment processes; additionally, MPC can handle process changes and disturbances, such as changes in influent quality and flow rate, by dynamically adjusting the control actions (Necoara, 2008). Thus, MPC is widely used in today's process industry due to its ability to handle constrained and multivariable control problems (Socha, 2007). For linear systems, the MPC problem is usually posed as a convex quadratic problem (QP), while for nonlinear systems one needs to solve a highly nonconvex optimization problem (DeCarlo, 1989).

ACADO Toolkit is a software environment and algorithm collection written in C++ for automatic control and dynamic optimization (Ariens et al., http://www.acadotoolkit.org). It provides a general framework for using a great variety of algorithms for direct optimal control, includ- ing model predictive control as well as state and parameter estimation. It also provides (stand-alone) efficiently imple- mented Runge-Kutta and BDF integrators for the simulation of ODE's and DAE's (Ariens et al., 2010). For the nonlinear MPC problem of the wastewater treatment process we use ACADO to solve the corresponding problem. However, since the problem is highly nonconvex, ACADO requires long CPU times to solve it. Hence, we propose an alternative where we linearize the system at each sampling time, we derive the corresponding linear MPC problem and solve it with a quadratic solver from Matlab. From simulations, we observe that the second approach is more efficient, since the closed loop behaviors are similar for linear and nonlinear MPC approaches, but the linearization based approach is faster in terms of CPU time than ACADO.

Nonlinear model predictive control

A nonlinear system is a system in which the change of the output is not proportional to the change of the input (Dasarathy, 1970). We write the nonlinear system that we work with as (Khalil 2002):

$$\dot{x} = f(x,u) \tag{1.11}$$

where $x \in \mathbb{X}$ and $u \in \mathbb{U}$. Thus, consider the following optimal control problem:

$$\min_{u(\cdot)} \int_0^T L(x,u)dt + V\big(x(T)\big) \tag{1.12}$$

subjected to the following equality constraints:

$$\dot{x} = f(x,u)$$
$$x(0) = x_0 \text{ given } x \in \mathbb{X} \text{ and } u \in \mathbb{U}$$

where the term $L(x,u)$ represents the stage cost, and $V(x(T))$ the terminal cost. In abstract terms, this is an optimization problem with constraints. For reference tracking, we consider the reference signals x^{ref} and u^{ref}. Then, $L(x,u) = \left\|x - x^{ref}\right\|_{Q_x}^2 + \left\|u - u^{ref}\right\|_{R_u}^2$ and $V\big(x(T)\big) = \left\|x_T - x_T^{ref}\right\|_{P_x}$. In order to simplify the algorithms we use, we approximate the nonlinear system that we work with by using the principle of Taylor series. We begin with a system of the form:

$$\dot{x} = f(x,u), x \in \mathbb{X}, u \in \mathbb{U} \tag{1.13}$$

Let $(\bar{x}, \bar{u})$ denote an equilibrium point, that is $f(\bar{x},\bar{u}) = 0$. Then, applying the Taylor series on the function f around the equilibrium point, we obtain (Socha, 2007):

$$f(x,u) \approx f(\bar{x},\bar{u}) + \frac{\partial f}{\partial x}(\bar{x},\bar{u})(x-\bar{x}) + \frac{\partial f}{\partial u}(\bar{x},\bar{u})(u-\bar{u}) \tag{1.14}$$

We denote $\delta x = x - \bar{x}$ and $\delta u = u - \bar{u}$ and we get the linearization $\delta \dot{x} = \frac{\partial f}{\partial x}(\bar{x}, \bar{u})\delta x + \frac{\partial f}{\partial u}(\bar{x}, \bar{u})\delta u$, which can also be written as:

$$\delta \dot{x}(t) = A_x \delta x(t) + B_u \delta u(t) \tag{1.15}$$

where $A_x = \frac{\partial f}{\partial x}(\bar{x}, \bar{u})$ and $B_u = \frac{\partial f}{\partial u}(\bar{x}, \bar{u})$. If the system is discretized using a sampling period ΔT, it can be written as (Jacod and Protter, 2011):

$$\delta x_{k+1} = A_x \delta x_k + B_u \delta u_k \tag{1.16}$$

Linear model predictive control

In general, a system with linear constraints over the states and inputs has the following form (Chen, 1984):

$$\begin{gathered} x_{k+1} = A_x x_k + B_u u_k \\ lb_x \leq x_k \leq ub_x, \forall k \in \{0, \dots, N-1\} \\ C_u u_k \leq d_u \end{gathered} \tag{1.17}$$

where $C_u \in \mathbb{R}^{n_i \times n_x}$ and $d_u \in \mathbb{R}^{n_i}$. Then, the optimal control problem for reference tracking is:

$$\begin{gathered} \min_{x_k, u_k} \frac{1}{2} \sum_{k=0}^{N-1} \left\| x_k - x_k^{ref} \right\|_{Q_x}^2 + \sum_{k=0}^{N-1} \left\| u_k - u_k^{ref} \right\|_{R_u}^2 + \left\| x_N - x_N^{ref} \right\|_{P_x} \\ x_0 = x, x_{k+1} = A_x x_k + B_u u_k \\ lb_x \leq x_k \leq ub_x, C_u u_k \leq d_u, \forall k \in \{0, \dots, N-1\} \end{gathered} \tag{1.18}$$

where x_k^{ref} and u_k^{ref} are certain reference values given for the state and control variables vectors of the system, over the prediction horizon, and the weighted norm has the following form:

$$\left\| v_k - v_k^{ref} \right\|_V^2 = \left(v_k - v_k^{ref} \right)^T V \left(v_k - v_k^{ref} \right)$$

Also, the matrices Q_x and R_u are both considered positive- semidefinite, $\forall k$.

The problem considered previously can be considered a convex quadratic optimization problem. To solve it, first we denote the decision variable as $x \in \mathbb{R}^{n_x + n_u}$ and write it as following (Necoara, 2013):

$$x = [u_0^T x_1^T u_1^T x_2^T \dots u_{N-1}^T x_N^T] \qquad (1.19)$$

The equality constraints of the optimization problem are linear and come from defining the dynamics of the system that is controlled. To formulate the quadratic problem, they can be concatenated in a single block constraint, taking into account the way in which the decision variable was defined. Mathematically, this means:

$$A_x = b, A \in \mathbb{R}^{Nn_x \times N(n_x+n_u)}, b \in \mathbb{R}^{Nn_x} \qquad (1.20)$$

The matrices A and b have the following form:

$$A = \begin{bmatrix} -B_u & I_{n_x} & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -A_x & -B_u & I_{n_x} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -A_x & -B_u & I_{n_x} \end{bmatrix}$$

$$b = \begin{bmatrix} A_x x_0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

This concatenation makes sense because the equations that describe the dynamics of the system over the entire prediction horizon can be written as:

$$\begin{aligned} & x_1 = A_x x_0 + B_u u_0 \Leftrightarrow -B_u u_0 + I_{n_x} x_1 = A_x x_0 \\ & x_2 = A_x x_1 + B_u u_1 \Leftrightarrow -A_x x_1 - B_u u_0 + I_{n_x} x_2 = 0 \\ & \vdots \\ & x_N = A_x x_{N-1} + B_u u_{N-1} \Leftrightarrow -A_x x_{N-1} - B_u u_{N-1} + I_{n_x} x_N = 0 \end{aligned}$$

The structure of the matrix A is a tridiagonal block, and the only nonzero term of the vector b depends on the initial state, which will be updated at each iteration of the algorithm. The inequality constraints can also be rewritten in the form of a single $Cx \leq d$ constraint. The inequalities corresponding to the states of the system can be written as:

$$\begin{bmatrix} I_{n_x} \\ -I_{n_x} \end{bmatrix} x_k \leq \begin{bmatrix} ub_x \\ -lb_x \end{bmatrix}$$

Therefore, the matrices $C \in \mathbb{R}^{N(2n_x+n_i)\times N(n_x+n_u)}$ and $d \in \mathbb{R}^{N(n_x+n_u)}$ have the following form:

$$C = \begin{bmatrix} C_u & 0 & 0 & \cdots & 0 & 0 \\ 0 & C_x & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & C_u & 0 \\ 0 & 0 & 0 & \cdots & 0 & C_x \end{bmatrix}$$

$$d \in \begin{bmatrix} d_u \\ d_x \\ \vdots \\ d_u \\ d_x \end{bmatrix}$$

Regarding the rewriting of the objective function in the standard convex QP form, a vector must be constructed with a structure similar to the decision variable x, but which concatenates the reference values over the entire prediction horizon. We denote it by x^{ref} and its form is as follows:

$$x^{ref} = \left[\left(u_0^{ref}\right)^T \left(x_1^{ref}\right)^T \left(u_1^{ref}\right)^T \left(x_2^{ref}\right)^T \dots \left(u_{N-1}^{ref}\right)^T \left(u_N^{ref}\right)^T\right] \tag{1.21}$$

If we also consider the diagonal matrix $Q \in \mathbb{R}^{N(n_x+n_u)\times N(n_x+n_u)}$, written as:

$$Q = \begin{bmatrix} R_u & 0 & 0 & \cdots & 0 & 0 \\ 0 & Q_x & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & R_u & 0 \\ 0 & 0 & 0 & \cdots & 0 & P_x \end{bmatrix}$$

then the cost function in the optimization problem can be rewritten as:

$$\begin{aligned} &\frac{1}{2}\|x - x^{ref}\|_Q^2 = \frac{1}{2}(x - x^{ref})^T Q (x - x^{ref}) \\ &\frac{1}{2}(x^T Q x - x^T Q x^{ref} - (x^{ref})^T Q x + (x^{ref})^T Q x^{ref}) \\ &\frac{1}{2} x^T Q x - x^T Q x^{ref} + \frac{1}{2}(x^{ref})^T Q x^{ref}. \end{aligned}$$

Next, we denote $q = -Qx^{ref}$ and by neglecting the term $\frac{1}{2}(x^{ref})^T Q x^{ref}$, we obtain the problem in convex QP form:

$$\min_{x\in\mathbb{R}^{N(n_x+n_u)}} \frac{1}{2}x^T Qx+q^T x$$
$$\text{s.t.}Ax=b, \quad Cx\leq d. \tag{1.22}$$

To further our research, we decided to reproduce the results obtained in ACADO by writing an algorithm in MATLAB. The goal is the same: stabilize the wastewater treatment system in the equilibrium points. Thus, we use linearization on the continuous system, then apply discretization, as shown in the following scheme:

Basically, we take the continuous system, transform it into a discrete one and then apply linearization. Mathematically, we have the following forms:

$$\dot{x} = F_c(x,u)$$
(1.23)
$$x_{k+1} = F_d(x_k,u_k) \tag{1.24}$$

We denote by F_c the continuous function and by F_d the discrete one.

The first step would be to discretize using the Euler method. Thus, we obtain:

$$x_{k+1} = x_k + \Delta T F_c(x_k,u_k)$$
(1.25)

Considering $x_{k+1} = F_d(x_k,u_k)$, we get that:

$$F_d(x,u) = x + \Delta T F_c(x,u) \tag{1.26}$$

The next step is linearization. The linear approximation of a function is the first order Taylor expansion around the point of interest. Therefore, we can write:

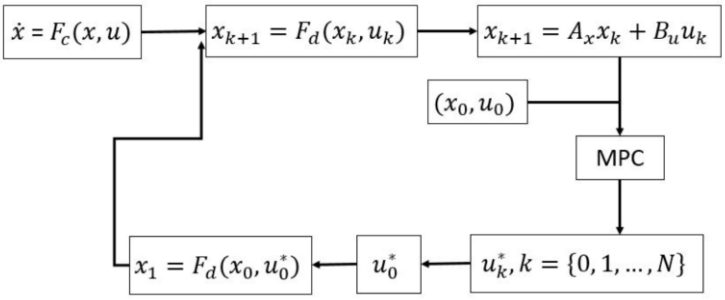
$$\begin{aligned}F_d(x_k,u_k) &\approx F_d(x_0,u_0)+\frac{\partial F_d}{\partial(x_k,u_k)}(x_0,u_0)\begin{bmatrix}x_k-x_0\\u_k-u_0\end{bmatrix}\\&=F_d(x_0,u_0)+\begin{bmatrix}\frac{\partial F_d}{\partial x_k}(x_0,u_0) & \frac{\partial F_d}{\partial u_k}(x_0,u_0)\end{bmatrix}\begin{bmatrix}x_k-x_0\\u_k-u_0\end{bmatrix}\\&=F_d(x_0,u_0)+\frac{\partial F_d}{\partial x_k}(x_0,u_0)(x_k-x_0)+\frac{\partial F_d}{\partial u_k}(x_0,u_0)(u_k-u_0).\end{aligned}$$

We denote:

$$A_x = \frac{\partial F_d}{\partial x_k}(x_0, u_0)$$
$$B_u = \frac{\partial F_d}{\partial u_k}(x_0, u_0).$$

Because $F_d(x, u) = x + \mathrm{h}F_c(x, u)$, the matrices can be also written as:

$$A_x = \frac{\partial(x + hF_c)}{\partial x} = I_n + h\frac{\partial F_c}{\partial x}$$
$$B_u = \frac{\partial(x + hF_c)}{\partial u} = h\frac{\partial F_c}{\partial u}. \tag{1.27}$$



$\dot{x} = F_c(x,u)$
$x_{k+1} = F_d(x_k, u_k)$
$x_{k+1} = A_x x_k + B_u u_k$
(x_0, u_0)
MPC
$u_k^*, k = \{0, 1, \ldots, N\}$
u_0^*
$x_1 = F_d(x_0, u_0^*)$

Fig. 1.8. Discretization and linearization scheme

Fig. 1.8. displays the discretization and linearization scheme for the predictive control.

A simplified mathematical model was used to describe the behavior of the wastewater treatment plan (Ghinea et al., 2023). The model has 4 state variables: X – biomass concentration, S – substrate concentration (the organic load), DO – dissolved oxygen and X_r – concentration of recycled biomass.

The ACADO Toolkit

ACADO practically applies optimal control on a nonlinear system. In order to do this, we consider the following cost:

$$
\begin{aligned}
&\min_{x_k,u_k} \frac{1}{2}\sum_{k=1}^{N} \|x_k - x_k^{ref}\|_{Q_k}^2 + \sum_{k=0}^{N-1} \|u_k - u_k^{ref}\|_{R_k}^2 \\
&\text{s.t.:} x_0 = x, \quad x_{k+1} = A_x x_k + B_u u_k \\
&\quad lb_x \le x_k \le ub_x \\
&\quad C_u u_k \le d_u, \quad \forall k = \{0,1,\ldots,N-1\}.
\end{aligned}
\tag{1.28}
$$

Here, x represents the states, $x = [X\ S\ DO\ X_r\ ]^T$ and u represents the control variable, $u = W$. Our purpose is to obtain values up to 40 mg/l for the substrate S, while keeping the values for the dissolved oxygen in the range $1 - 3$ mg/l. Moreover, the input variable, W, must be kept under 100 m^3/h. Thus, we consider the input constraint $0 \le u \le 100$, the output constrain $0 \le y \le 40$ and the state constraint $1 \le x(3) \le 3$. In this way, the quality of the water is obtained in accordance with national standards in the field, while maintaining a reasonable consumption of electricity. This consumption, which is the main consumption in the case of wastewater treatment plants, is determined by the blowers used for aeration.

In ACADO,we create a matrix Q that contains Q_k and R_k from the cost above, $Q_k = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $R_k = 1$. Basically, we want to stabilize our system using the state S and the control variable W. This means that the cost we consider has roughly the form $\min_W \int S^2 + W^2$. All that remains is for us to choose the equilibrium points for the system. We also consider the value for the stepsize as $\Delta T = 0.5$.

We consider two sets of equilibrium points:

Case 1. *rr* = [223.8 38.9 2.6 447.6 33].

Case 2. *rr* = [228.7 37.1 2.9 457.4 35].

We observe that both the states and the control variable reach the values we wanted to obtain, no matter what equilibrium points we set.

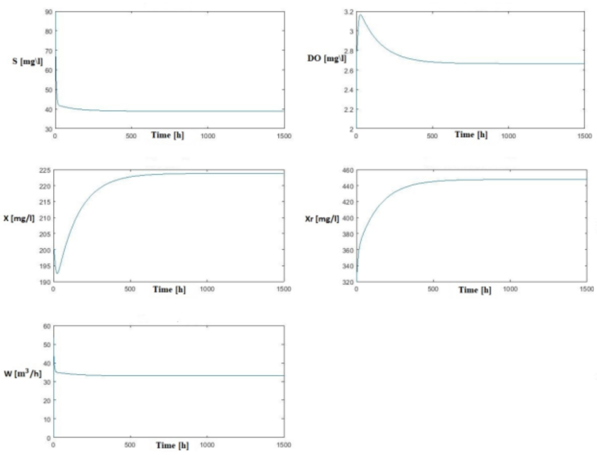


Fig. 1.9 ACADO simulations for Case1

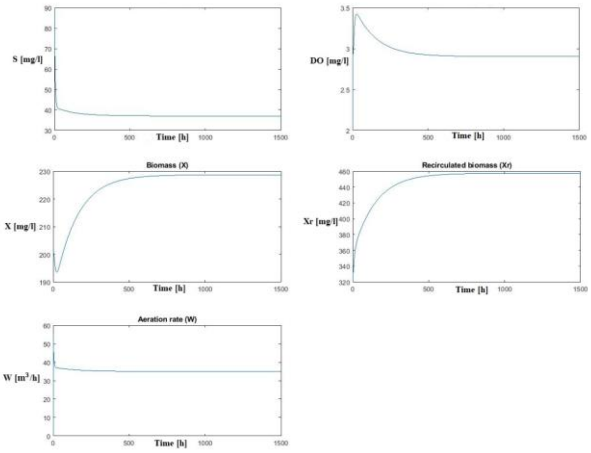


Fig. 1.10 ACADO simulations for Case2

In Matlab, we simulate the optimization problem for the following form:

$$x_{k+1} = A_x x_k + B_u u_k + a$$

where $a = F_c(x_0, u_0) - A_x x_0 - B_u u_0$.

In order to do this, we first build a function that calculates the matrices that we denote A_x and B_u using (1.27), then use these two matrices, as well as $Q_x = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $R_u = 1$ that we used in ACADO (since the cost is the same) in another function that creates the elements needed for the sparse QP form. This second function results in the elements Q, q, A, b, C, d that make up the following QP form:

$$\min_{\psi} \frac{1}{2} \psi^T Q \psi + q^T \psi \tag{1.29}$$

with the constraints $A\psi \leq b$ and $C\psi \leq d$.

In the script that calls these functions we first initialize the states and control variables as $x_0 = [200; 90; 2; 320]$ and $u_0 = 30$. Then, according to the scheme in Figure 1.8, we compute u_k^*, $k = \{0,1,\ldots,N\}$ using either the command *quadprog* (a solver for quadratic objective functions with linear constraints), or the Matlab Software CVX (a Matlab-based modeling system for convex optimization; CVX turns Matlab into a modeling language, allowing constraints and objectives to be specified using standard Matlab expression syntax). Whichever of these two we decide to use, the next steps are the same.

We use only the first element of u_k^*, $k = \{0,1,\ldots,N\}$, that is u_0^*, then we compute the next value for the state vector, x_1 using the discreet function F_d calculated in the current value for x, that is x_0 and u_0^* that we have just found. All that remains is to set x_0 and u_0 that are going to be used for the next iteration:

$$x_0 = x_1$$
$$u_0 = u_0^*$$

Just like with ACADO, we give $\Delta T = 0.5$ and run the program for the same two cases of equilibrium points.

We observe that both the states and the control variable reach the values we wanted to obtain, independent of the equilibrium points we set.

To conclude, we compare the values we obtained with ACADO Toolkit and with the Optimal Control algorithm we created:

Concerning CPU time, the algorithm we built in Matlab is much faster than the one we created with ACADO Toolkit (200 seconds versus 2 full days). When it comes to stabilization, it is clear from the graphics in the previous section that the algorithm in ACADO stabilizes faster than the Optimal control one; both algorithms are able to reach the equilibrium points for the states and control variable we set for them to obtain.

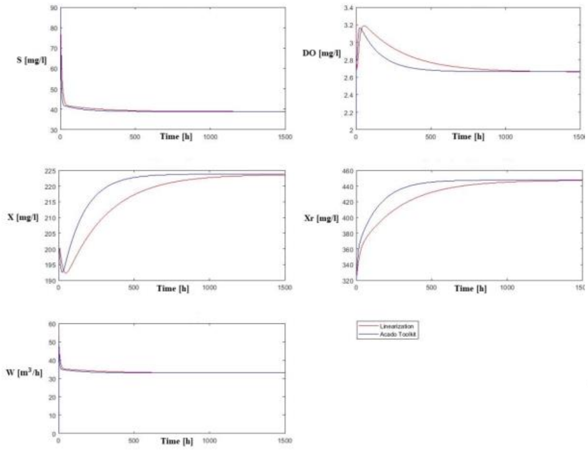


Fig. 1.11 ACADO vs. Linearization for Case1

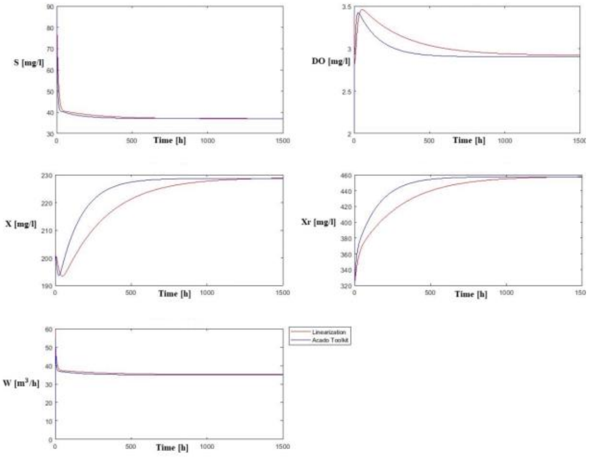


Fig. 1.12 ACADO vs. Linearization for Case2

1.3.Process Surveillance and Control in Membrane Treatment Processes

Large, available data and the rapid improvement in computational power have alleviated the recent progress in numerical optimization models allowing optimization in hyperdimensional spaces where analytical solutions are too expensive.

The future of digitalization of membrane material design and optimization is an AI-enabled structure reconstruction and generation, prediction of properties and in-service performance for membrane materials.

MBR process has two main drawbacks: membrane fouling and high energy consumption. Most of the energy required is for air scouring. Membrane fouling prevention and energy consumption in MBR can be balanced by:

- monitoring the permeability of the membranes in real-time
- regulating the air scour flow accordingly

It can be obtained an average reduction in the air scour flow rate of 13% - 20%, corresponding to 14 - 22% energy saving (SmartAirMBR).

Dynamic ultrafiltration enables to mitigate fouling issues and allows operation with higher fluxes than conventional crossflow operation. However, fouling is not fully avoided, so a flux estimation is required for determining the best operation scenarios. Due to the limited dynamic system understanding, machine learning models are proposed. Machine learning methods applicable: neural networks, decision trees, random forest, regression Gaussian processes and classical methods such as space-state and ARMAX (Autoregressive Moving Average with Exogenous Inputs). The novelty of the approach lies in the proposed combination of several models to achieve a prediction with low uncertainty.

The selection of optimal materials can be done through machine learning. Machine learning can predict inherent membrane parameters (rejection or flux) using only molecular structural information. Molecular structural information of the solutes, solvents, and membranes can use for interpretation of features of the solute, solvent, and membranes affect the rejection and flux. Using graph neural networks, modifying effect of functional groups, rings, or even single bonds and atoms in a molecule – leading to optimal structures. A database (www.osndatabase.com) shows features of over 500 different chemical compounds in 10 different solvents and four different membranes and some models.

Polymer chemistry plays a vital role in membrane separation performance, processability in solvents, and ability to selectively capture gases like CO_2. The performance parameters can be variables such as the solubility, diffusivity, permeability, ideal and multicomponent selectivity, swelling and miscibility in common solvents. Machine learning based systems for faster screening can work even with very limited information like molecular chemistry.

Porous energy materials are essential components of many energy devices and systems, the development of which have been long plagued by two main challenges:

- the “curse of dimensionality”, i.e. the complex structure–property relationships of energy materials are largely determined by a high dimensional parameter space.
- low efficiency of optimization/discovery techniques for new energy materials

The solution is the digitalization of porous energy materials, transforming all material information into the digital space using reconstruction and imaging data and fusing this with various computational methods. The rapid characterization, the prediction of properties, and the autonomous optimization of new membrane materials can be achieved by using advanced mathematical algorithms combined with various ANN tools.

Membrane fouling detection/prediction can be done by spectroscopic fingerprinting. Online monitoring of fouling potential enable smart control for managing fouling. The spectroscopic methods are likely to be a key concept, but indicators are not yet defined. 11 UV-Visible indicators, 19 Fluorescence Emission-Excitation Matrix (FEEM) and 2 infrared scattering indicators were scanned during a 151 days period. The membrane pore blocking and gel/cake fouling potential were found to be well correlated with UV-VIS and 15 FEEM. UV-VIS and FEEM scanning can be integrated in a model to predict and detect fouling. Real-time scanning of UV-VIS and FEEM now enables faster and even real-time detection.

Early-warning protocol for membrane cleaning by predicting, diagnosing, and producing warnings (e.g. biofouling phenomena in MBR plants) can be implemented. Biofouling progress was recursively predicted utilizing Kalman filter method – to identify the dominant fouling mechanism, incorporating genetic algorithm. Membrane cleaning warning rule based on fouling cumulative sum control chart – alarms for operational failure in the targeted plant.

2. Virtual Sensors

2.1.Integration of ANN for Accurate Estimation and Control in Wastewater Treatment

The current study centers on the deployment of an ANN-based Soft Sensor for the purpose of forecasting pollutant concentrations in WWTPs. The primary aim of the soft sensor under consideration is to facilitate control strategies by ensuring that the levels of pollutants remain within the prescribed limits. The precise prediction of effluent limit violations and the proactive mitigation of their consequences can lead to a reduction in operational expenses and an improvement in overall performance for wastewater treatment plants.

The ongoing research involves the utilization of an Artificial Neural Network (ANN) for a specific application. The inputs to the ANN comprise the influent and effluent measurements of the Wastewater Treatment Plants (WWTPs) collected over a period of one year, with a sampling interval of 15 minutes. The measurements were acquired through the utilization of the BSM2M, using a computer-simulated model of a versatile wastewater treatment plant (see Fig. 2.1). The structure of the plant is identical to that of the wastewater treatment plant in Galati city. More comprehensive understanding of the issue can be found in (Satin et al., 2016; Pisa et al., 2021; Pisa, 2022).

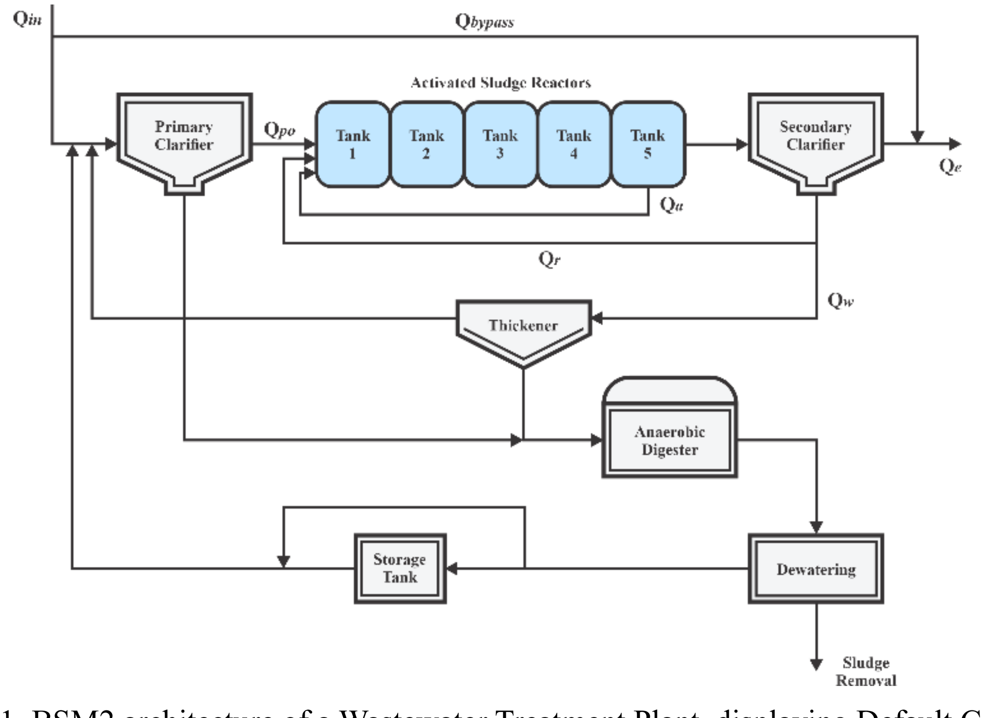


Fig. 2.1. BSM2 architecture of a Wastewater Treatment Plant, displaying Default Control strategies. Q_{po} represents the primary clarifier overflow, Q_a and Q_r the internal and external recirculation fluxes, and Q_{in} and Q_e the influent and effluent, respectively.

In Fig.2.2, we illustrate the problem under investigation. The inputs to the system comprise influent and available measurements obtained from the WWTPs. These measurements include water flows and nutrient concentrations, such as the ammonium concentration in the fifth bioreactor tank ($S_{NH,5}$), the output flow from the first clarifier (Q_{po}), the environmental temperature (T_{as}), and the total suspended solids (TSS) (Barbu et al., 2018). The main goal employs an ANN to predict the effluent concentrations ($\hat{y}_t$). The inputs chosen for this application are analyzed to determine their predictive capabilities. It relies on a prediction methodology that involves the utilization of two-stacked Long-Short Term Memory (LSTM) cells.

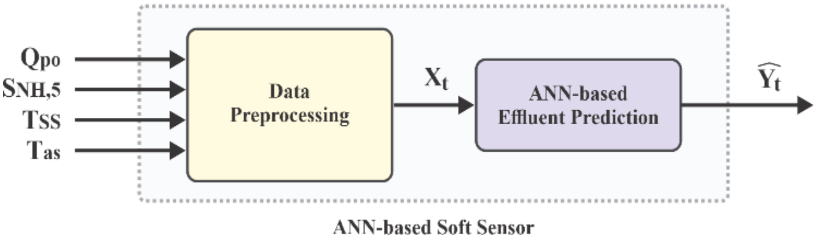


Fig. 2.2. Artificial Neural Network (ANN)-based Soft Sensor. The data used for input and output are representative of the influent and effluent measurements, respectively.

These cells are a type of artificial neural network that is characterized by its gating mechanism. As per the research findings presented in references (Goodfellow et al., 2016; Pisa, 2022), every LSTM cell is comprised of 75 hidden neurons per ANN that is contained within the cell.

The analysis is centered on the examination of ammonium ($S_{NH,e}$) concentrations, which are among the most commonly occurring pollutant nutrient concentrations detected in wastewater treatment plants (WWTPs). Infrequent occurrences of peaks in ammonium ($S_{NH,e}$) concentrations have been observed. The prediction task carried out by the Soft Sensor based on ANNs presents a significant challenge due to the infrequent incidence of these events and the imbalanced distribution of the data.

Data preparation

The optimization of performance and reduction of complexity in Artificial Neural Networks (ANNs) are heavily reliant on the implementation of data preprocessing techniques (Naduvil-Vadukootu et al., 2017). The issue of imbalanced data within industrial processes presents a challenge for conventional approaches when dealing with regression problems. In order to address these challenges, a new approach to data preprocessing has been developed. This innovative set of mechanisms will be thoroughly examined in the subsequent sections, where their unique features and benefits will be outlined in detail.

A. Sliding Window

We propose implementing a novel sliding window methodology to improve the arrangement and maintain the temporal coherence within the dataset. The present methodology incorporates two fundamental variables, namely the window length (WL) and the prediction horizon (PH). In the present study, the configuration of WL and PH was established as follows:

- A Window Length (WL) of 10 hours has been selected as an appropriate time frame to retain the values observed at each sampling time and encompass the preceding measurements. This approach is aimed at capturing a broad historical context of the data being analyzed.

- A Prediction Horizon (PH) of 4 hours has been considered. This parameter defines the period during which predictions of effluent concentrations can be provided beforehand, thus facilitating proactive decision-making.

The utilization of the sliding window mechanism in an ANN system enables it to effectively incorporate both current and past measurements, thereby leveraging the significant temporal correlation present in the data.

The sliding window technique is implemented in such a way that a novel measure is generated with every movement of the window, while the oldest measure is removed in accordance with the First-In-First-Out (FIFO) principle. As illustrated in Fig. 2.3, the system assimilates the preceding 10-hour recorded data for each novel measurement. The architectural specifications of the considered WWTP have determined the retention time requirements to be 14 hours. The specific configuration of the sliding window parameters has been analyzed to meet these requirements. Further insights into the underlying architecture can be found by referring to reference (Satin et al., 2016).

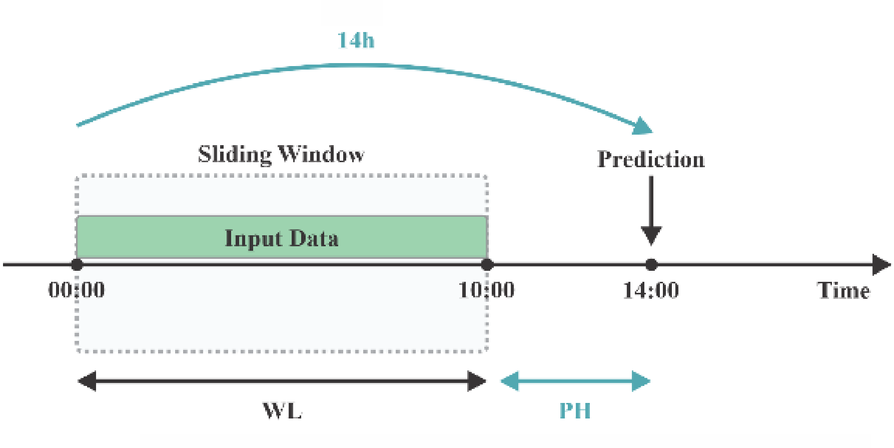


Fig. 2.3. Structure of the Sliding Window. The WWTP holding time is the same as the sum of the Window Length and the Prediction Horizon.

B. Data Normalization

We propose the utilization of data normalization techniques as a potential solution to address the issue of data heterogeneity. The Z-score adjustment method is one way we do this. When rare events happen, the latter can be prone to bias (Garcia et al., 2015). The Z-score normalization process is computed as follows:

$$x_t = \frac{x - E[x]}{\sqrt{E[(x - E[x])^2]}} \tag{2.1}$$

It shows the data that needs to be normalized and the data that has been normalized. By using this normalization method, we hope to standardize the way the data is spread out and lessen the effect of extreme values, making the ANN's input more fair.

C. K-Fold Based Training

When working with large time series datasets, it is not uncommon to encounter imbalanced data, and effluent signals are a prime example of this disparity. Failure to address the issue of imbalanced data can result in biased predictions that favor the more frequently represented values, particularly those falling below certain thresholds (Bergmeir et al., 2018).

To tackle this challenge, K-Fold has emerged as a viable data preprocessing technique during the learning stage (Barbu et al., 2018). This approach operates based on two fundamental principles: dividing the dataset into equally sized subsets and the execution of training processes. In our specific case, the dataset comprises the influent and effluent measurements from the BSM2 model of WWTP.

The number of 5 K-folds has been carefully chosen to allocate 70% of the complete dataset for training the ANNs while reserving 30% for testing and validation purposes. Within this 30%, 15% is designated for validation, while the remaining 15% serves as the test subset. The objective is to obtain distinct prediction models through each training process, resulting in a total of models. The dataset is utilized for each model, with subsets employed for training and one subset dedicated to testing and validation.

Ultimately, the model that exhibits superior prediction accuracy among all training processes is selected for the final application. A visual depiction of the K-Fold methodology is presented in Fig.2.4.

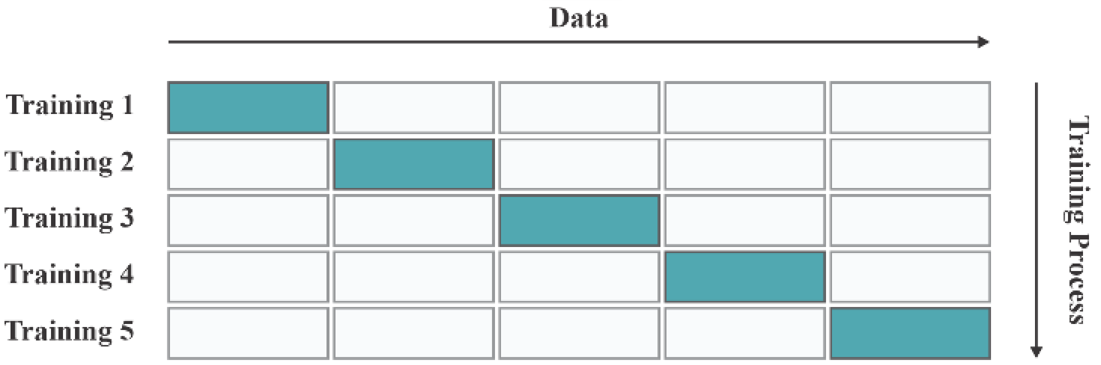


Fig. 2.4. K-Fold method, a commonly used technique in machine learning for model validation and selection. colored data.

Evaluation of the soft sensor

The performance evaluation (Fig. 2.5) of the proposed data preprocessing techniques for time-series industrial data relies on the predictions generated by the ANN-based Soft Sensor. The present study utilizes three distinct metrics to evaluate the performance of the model. These metrics include Root Mean Squared Error ($RMSE$), Mean Absolute Percentage Error ($MAPE$), and Coefficient of Determination (R^2).

The RMSE is a commonly used metric in statistical analysis to measure the difference between predicted and actual values. It is calculated using the following formula:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y_i})^2} \tag{2.2}$$

where $\widehat{y}_i$ represents the ith prediction of the effluent concentration and y_i denotes the corresponding target value. A lower RMSE value indicates accurate predictions.

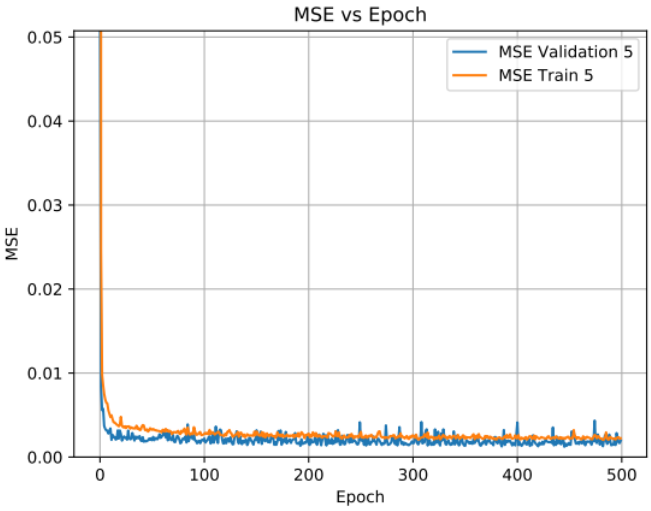


Fig. 2.5. The performance assessment of the fifth k-fold, displaying the ideal outcome for the applied data set (ANN with TSS), and the optimal MSE values for our data.

The MAPE is another commonly used metric in the field of predictive modeling. It is calculated by taking the mean of the absolute percentage errors in the prediction process:

$$MAPE = \frac{1}{N}\sum_{i=1}^{N}\left|\frac{y_i-\widehat{y}_i}{y_i}\right| \cdot 100 \tag{2.3}$$

This metric is often preferred over other error metrics as it provides a more intuitive understanding of the accuracy of the model.

The coefficient of determination, commonly known as R^2 is a statistical measure that evaluates the ability of an ANN model to account for the variability observed in the data. This metric quantifies the proportion of the total variation in the dependent variable that can be explained by the independent variables included in the model. The calculation is derived through the utilization of a specific formula:

$$R^2 = \frac{(\sum_{i=1}^{N}\left(\widehat{y}_i-\overline{\widehat{y}}\right) \cdot (y_i-\overline{y}))^2}{\sum_{i=1}^{N}(\widehat{y}_i-\overline{\widehat{y}})^2 \cdot \sum_{i=1}^{N}(y_i-\overline{y})^2} \tag{2.4}$$

The symbol $\overline{\widehat{y}}$ represents the mean of the predicted values and $\overline{y}$ denotes the mean of the target values. This notation is commonly used in statistical analysis and machine learning models.

The combination of these metrics offers a thorough assessment of the effectiveness of the Artificial Neural Network (ANN) based Soft Sensor.

The results of the evaluation indicate that the ANN model exhibits remarkable accuracy in its predictions. The present study has developed a model that is capable of accounting for approximately 97% of the data variance, as indicated by the R^2 value. This high level of variance accounted for by the model has resulted in precise predictions, which are further supported by the low values of RMSE and MAPE. Specifically, the ANN model has yielded RMSE and MAPE values of 0.048 and 3.54%, respectively. These findings suggest that the developed model is highly accurate and reliable in predicting the outcomes of interest. The precision of the predictions is demonstrated in Fig. 2.6 and Fig. 2.7, despite the presence of some unfavorable predictions, where the ANN displays remarkable accuracy in predicting S_{NH} values. The present study highlights that the aforementioned enhancements are predicated on prognostications derived from the complete one-year dataset as input.

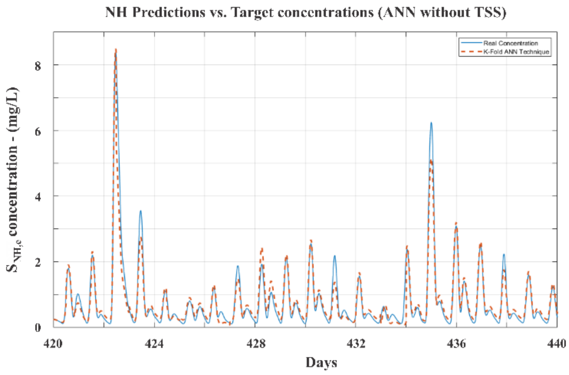


Fig. 2.6 $S_{NH,e}$ predictions using the ANN-based Soft Sensor and K-Fold implementation, not taking into consideration the TSS for the trained ANN.

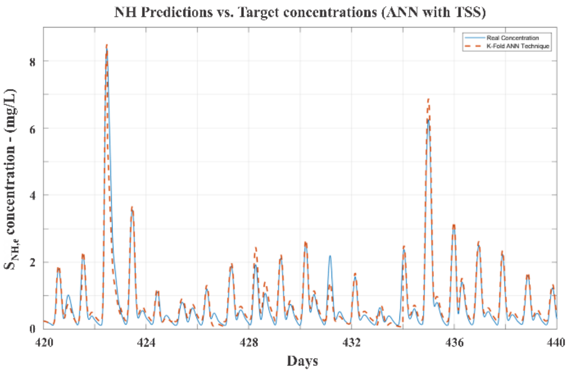


Fig. 2.7 $S_{NH,e}$ predictions using the ANN-based Soft Sensor and K-Fold implementation, also considering the TSS as an input (Fig.2.2).

2.2.Achieving legislative requirements in wastewater treatment using digital tools

The Urban Wastewater Treatment Directive (UWWD) requires member states to remove phosphates and organic matter from domestic wastewater depending on the size of the wastewater treatment plant (WWTP) and the environmental sensitivity of the location (Council Directive 91/271/EEC of 21 May 1991). Organic matter in wastewater, which is commonly measured as Chemical Oxygen Demand (COD) or Biochemical Oxygen Demand (BOD), can be efficiently removed with biological wastewater processes. While the chemical treatment process- coagulation- is extremely efficient in removing phosphates, it does not remove the dissolved fractions of COD/BOD in wastewater (Ratnaweera and Fetting, 2015). This has caused a big challenge for WWTPs which do not have biological stages.

Although Norway is not a member of the EU, it obliges to fulfil the requirements of the UWWD. 23% of the population of Norway is connected to chemical, 42% to chemical-biological and only 9% to pure biological WWTPs (https://www.ssb.no/en). This has caused extensive discussions on the fulfilment of the EU UWWD, and as an intermediate measure, Norwegian environmental authorities have permitted their WWTPs not to focus on the COD/BOD removal requirement. However, in recent years, this practice was changed and all WWTPs above 10 000 pe are now required to follow the EU UWWD.

The UWWD requires >75% removal or <125 mg/l COD in effluent and >70% removal or<25 mg/l BOD in effluent (Council Directive 91/271/EEC of 21 May 1991). Since the coagulation can remove on the suspended fraction of COD/BOD and that fraction is usually 40-60%, the general perception is it is impossible to achieve the UWWD requirements. The consequence is expanding the existing Norwegian WWTPs with biological stages, which will cost hundreds of millions of Euros.

Although the pure suspended fraction, which is measured as Suspended solids (SS) larger than 1 µm, coagulation may efficiently remove colloids, which are larger than 10 ηm. This may open new possibilities to have an extended removal of COD/BOD reaching the required removal levels.

During the coagulation process, an inorganic salt, often aluminium or iron, is added to the wastewater. The resulting hydrolysis process with phosphates removes colloids and particles while the chemical reactions remove phosphates.

The efficiency of the coagulation process critically depends on the coagulant dosage, which has to be optimal for the influent water quality at all times, which changes rapidly during the day. And the optima coagulant dosage depends on the flow of wastewater, its pH, particles, and phosphates content. Nevertheless, only the incoming flow is considered in practice when calculating the dosage, sometimes with overriding pH to secure an optimal hydrolysis process. This practice result in suboptimal results due to under- or overdosing.

Although the need to consider particles and phosphates in addition to the flow and pH is well acknowledged, the lack of affordable and accurate sensors to measure these parameters in real-time as well as the lack of efficient conceptual models for wastewater coagulation has prevented implementing them.

This paper presents the experience with the use of surrogate systems to monitor water quality and use them in process control to achieve COD/BOD requirements in a coagulation plant eliminating the need for expanding with a biological stage.

Process Description

Full-scale experiments were carried out at the Søndre Follo WWTP (SFR) in Vestby which is situated 60 km south of Oslo. SFR treats wastewater from 24 000 persons and treats 3500-9000 m3/day, depending on the weather/precipitation. The current discharge permit required >90% removal of total-Phosphates while the plan must achieve the secondary treatment requirement. The SFR is a mechanical-chemical treatment plant.

The plant has installed several physical online sensors measuring the flow, suspended solids, conductivity, pH temperature in the inlet, pH after coagulation, and suspended solids after sedimentation (effluent). Surveillance data are collected every 10 minutes and stored in the SCADA system. total-P were measured daily average samples at the WWTP and weekly by accredited laboratories. COD and BOD were measured in 24 daily samples by accredited laboratories annually as required by the legislation. These data were supplemented by several sampling campaigns which measured hourly samples during dry and wet weather and on weekdays and weekends at the DOSCON laboratory. Samples were analyzed using Norwegian Standard Methods. Analytical results were cross-validated using several analytical methods.

The analytical data were used to calibrate hybrid soft sensors for total-P and total-COD and total-BOD using a concept presented by (Nair et al., 2022). The surveillance data from physical sensors and soft sensors were integrated and used for further analysis.

The coagulant dosing was determined using a concept developed by DOSCON, using multivariate statistics combined (Manamperuma et al., 2017) which was further improved using Artificial Neural Networks. The concept considers all critical parameters critical for the coagulation process unlike the commonly used flow proportional dosing with pH overriding, thus particles and phosphates are directly or indirectly included.

Accuracy of the software sensor

Although the DOSCON concept secured >90% removal of phosphates, SFR's performance referring to organic matter (COD and BOD) was not in compliance with the legislation. To further optimize the COD/BOD removal, we considered integrating total-P and total-COD surveillance in the algorithms for coagulant dosing.

Figs 2.8 and 2.9 present the model accuracy for hybrid sensors for total-P and total COD. In these figures, we use R^2 as an indicator for the accuracy of the prediction against measured values (True data). The predictions were satisfactory considering the wide variations in the influent wastewater quality.

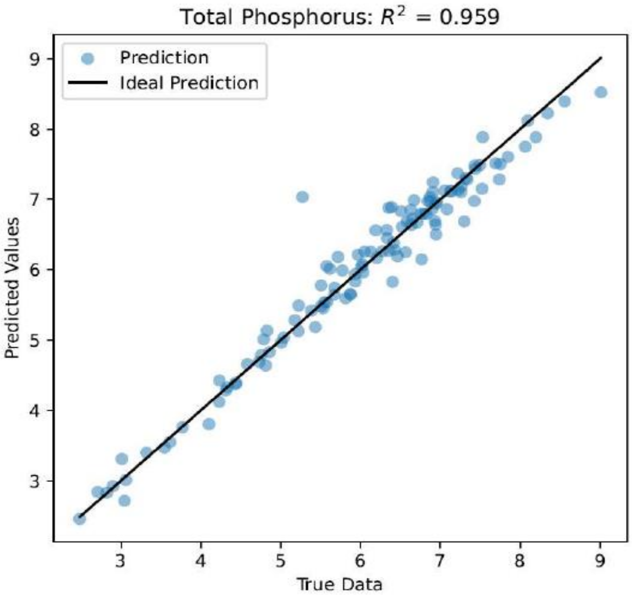


Fig 2.8. Model accuracy of the prediction of Total-P

With further tuning of the dosing algorithms, the plant has recorded performances complying with the secondary treatment requirements, as presented in Figs 2.10, 2.11, and 2.12, for total-P, COD, and BOD respectively.

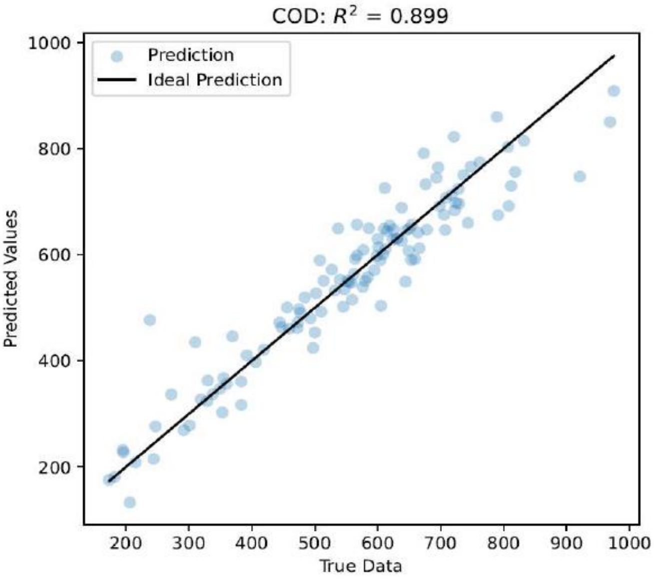


Fig 2.9. Model accuracy of the prediction of total-COD

The model accuracies obtained for the two parameters were considered satisfactory and were integrated into further optimization of the coagulant dosing determination.

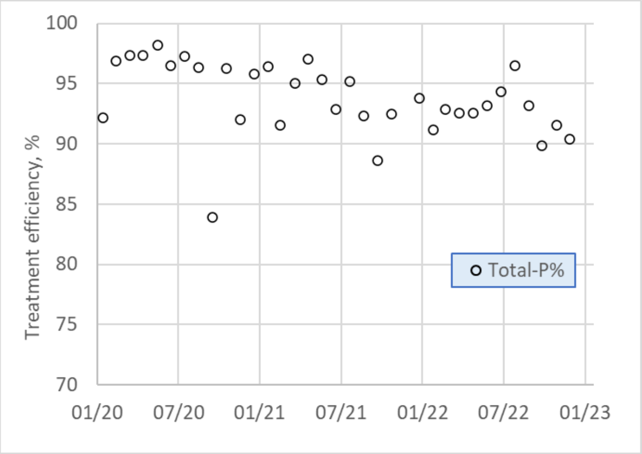


Fig 2.10. Removal efficiency of Total-P. Compliance requirement >90%

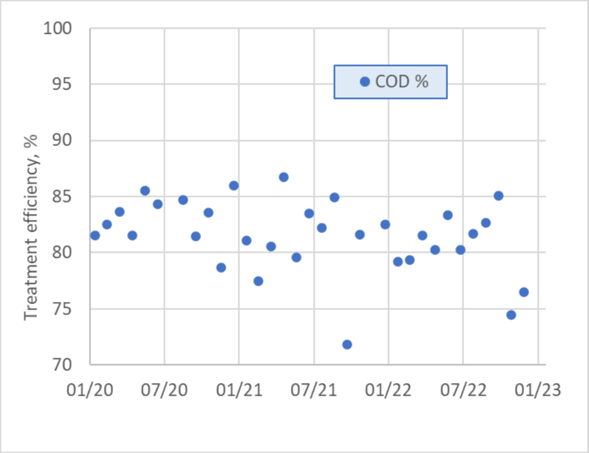


Fig 2.11. Removal efficiency of COD. Compliance requirement >75%

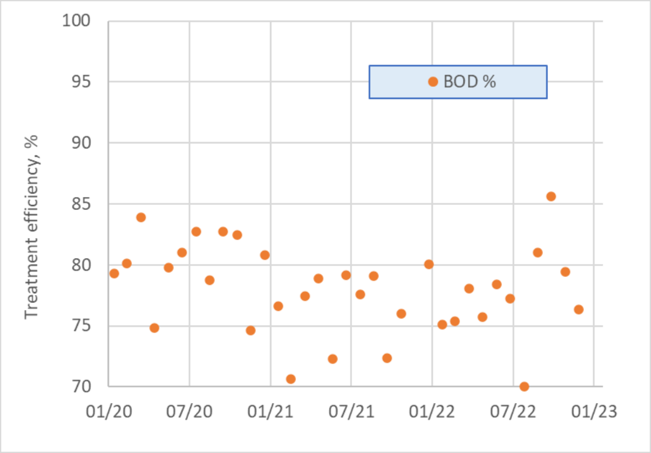


Fig 2.12. Removal efficiency of BOD. Compliance requirement >70%

Influent and effluent water quality vary rapidly during the day and only with real-time measurements, one can respond swiftly to address any performance weaknesses. Therefore, it is valuable to have real-time surveillance regarding the compliance parameters, such as total-P, COD, and BOD. While there are physical sensors for COD are available in the market, there are no similar sensors for phosphates. The only near-real-time option was to use online analysers. Such equipment is quite expensive (15 000-50 000€ each), while hybrid soft sensors provide a good alternative for a fraction of the cost. Figs 2.8 and 2.9 confirm the validity of the models used in soft sensors and provided comparable results with the accredited lab values.

Fig 2.8 presents the accuracy of the soft sensor model for Total-P, which seems good. Fig 2.9 presents the accuracy of the COD soft sensor model. Although it is not as good as the Total-P model, it serves the purpose of optimizing the COD removal efficiencies. The weaker model accuracy is a result of limited surveillance data available for calibration of the model, and with the growth of surveillance data, the model is becoming better and more robust.

The soft sensors are integrated into the operational real-time dosage estimating algorithms. Instead of having suspended solids as the target parameter, Total-P was introduced. Fig 2.10 presents the compliance reporting values for Total-P, twice per month, over 2 years. They are well above the compliance levels (>90%), except for occasional lower values, which are also permitted. Further investigation on these exceptional conditions revealed that they are either due to extraordinary inflows drastically reducing the sedimentation times or/and plant maintenance activities.

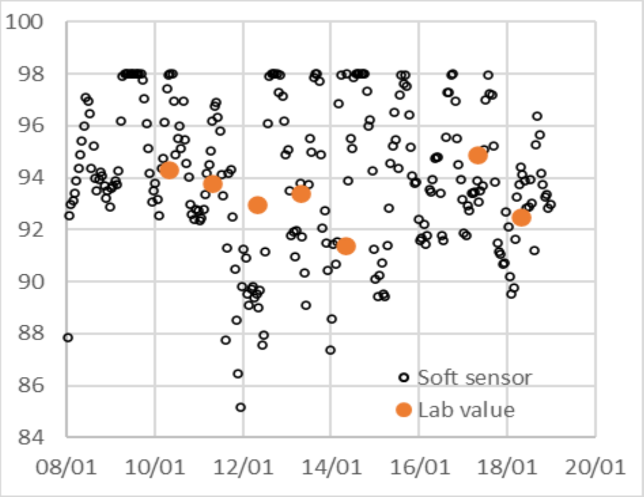


Fig 2.13. Removal efficiency of Total-P with real-time values

Fig 2.13 presents the real-time data for Total-P for 12 days, compared with lab values. The real-time values from soft sensors revealed that the treatment efficiency could vary between 85-98% to result in 91-95% average results. These values were continuously displayed at the WWTP making operators to be more aware of the conditions, while the modeling team could work more concretely on reducing events with far below compliance events. The work is still ongoing to eliminate both too-low and too-high treatment efficiencies, and real-time surveillance and virtual soft sensors enable this process.

Fig 2.11 presents the COD removal efficiency over 2 years, based on compliance reporting. The compliance requirement is either >75% removal or <125 mg/l in the effluent. Fig 5 presents similar results for BOD. Apart from two occasions over two years, COD results were within compliance levels while all BOD values were within the limits.

The general perception is that achieving the secondary treatment requirements for organic matter removal is impossible to realize only with coagulation. However, the above-presented results document the capability of achieving the compliance requirements in a mechanical-chemical plant. When the suspended fraction of COD and BOD are normally <60%, achieving >75% and 70% respectively, deserved further elaboration on the underlying mechanisms.

Coagulation removes not only the suspended fraction (>1µ) but also the colloidal fraction (0.1-1µm). Thus, it is reasonable to assume also the colloidal fraction of COD and BOD will be removed during coagulation. We have not yet analyzed the colloidal fraction of COD in the wastewater from SFR WWTP, but the analysis from the literature is provided in Table 2.1.

Table 2.1. COD Fractions Reported in Other Studies

Total COD	**Suspended COD**	**Colloidal COD**	**Dissolved COD**	**Colloidal + suspended**	**Reference**
699	409	71	219	69 %	(Tawfik et al., 2010)
733	485	64	185	75 %	
803	603	49	151	81 %	

334	137	39	80	76 %	(Drewnowski et al., 2020)
650	413	24	213	67 %	
630	442	36	152	76 %	
590	408	39	143	76 %	
548	384	33	131	76 %	
451	313	32	106	76 %	
821	630	37	154	81 %	
620	444	44	132	79 %	
1390	1143	73	174	87 %	
1001	765	64	172	83 %	
797	632	53	112	86 %	
750	558	44	148	80 %	

According to the data presented in Table 2.1, the total suspended and colloidal fraction of wastewater could reach even 87%. Thus it seems logical to expect >75% removal of COD.

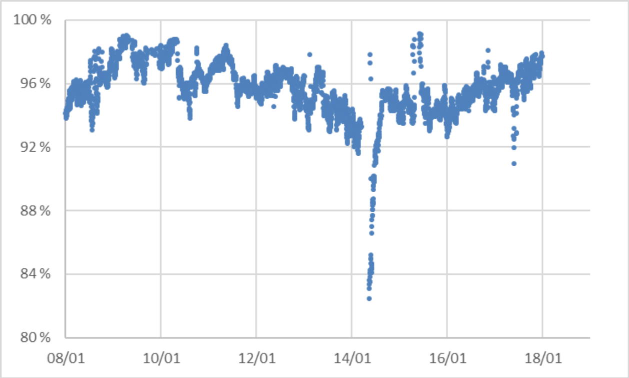


Fig 2.14. Removal efficiency of Suspended solids with real-time values

However, even after a comprehensive destabilization process with coagulation, the final removal of the said fraction will depend on the comprehensiveness of the separation process. Even in well-functioning situations, the removal rates for suspended solids varied between 92-98%. Fig 2.14 presents the suspended solids removal efficiencies at SFR WWTP, which shows the removal efficiency varied between 91-99% except for a shorter period with 82%. Thus, to secure >75% removal of COD, it is, therefore, necessary to have suspended + colloidal fractions of well above 80%.

The dosing control algorithm at the SFR WWTP is based on inlet and outlet-suspended solids. Considering the reflections on the removal of colloidal fractions in addition to the suspended fraction, we may then anticipate an even better prediction of the optimal dosage, if both fractions can be considered. However, real-time measurement of colloidal fractions of particles or organic matter with physical sensors is not realistic at present. Nevertheless, we believe that it would be possible to estimate it using a hybrid soft sensor. Particles in wastewater are measured both as turbidity and suspended solids, thus there could be a possibility to derive an estimate for the sum of colloidal and suspended fractions using a combination of these two parameters supplemented with other physical sensors in developing a hybrid soft sensor. Whether it would be possible to derive the total colloid and suspended fraction only with a suspended solids sensor and a turbidity sensor is also an interesting question, which needs to be elaborated on in the future.

3. Analysis of the Cybersecurity Incidents in the Water Sector

Water utilities are essential for health, safety and well-being, and they are considered as critical infrastructures (CIs) whose disruption of service can lead to significant loss from economic, public safety and environmental standpoints (Igure et al., 2006; Moraitis et al., 2020). Supervisory Control and Data Acquisition (SCADA) systems provide monitoring and control capabilities for real-time operations of the water utilities (Rasekh et al., 2016) . In the past, SCADA systems relied on air-gapped networks and non-standard protocols to protect them from cyberattacks (Igure et al., 2006). Currently, these networks have been connected to corporate networks and the internet. There have also been advances in using standard networking protocols for communications (Cheung et al., 2006). These changes have made SCADA systems more available for attackers to target remotely through the Internet from anywhere in the world (Christiansson and Luiijf, 2008).

Although the integration of the SCADA and corporate networks has significantly improved the efficiency of the systems, it has also increased the attack surfaces and has exposed both physical and cyber infrastructures to attacks (Housh and Ohar, 2018; Ramotsoela et al., 2019; Rasekh et al. 2016). For example, a successful attack in the water sector can lead to chemical contamination, physical damage, or communications disruption between the network elements and the SCADA system. Several cyberattacks such Harrisburg water plant (2006), Northern Colorado water system (2019), Israel's water system (2020), Florida wastewater (2021) (Sharmeen et al., 2021) exemplify the cybersecurity issues facing the water sector. The number of reported cyberattacks on the water sector is growing and making them the third most targeted sector (ICS-CERT 2016).

Understanding the various dimensions of these cybersecurity incidents and how they have evolved over time can provide insight for developing effective strategies to prevent or mitigate similar attacks in the future (Miller and Rowe, 2012). Hassanzadeh et al., 2020 reviewed cybersecurity incidents in the water sector. While their study contributes significantly for helping to understand the nature of cybersecurity incidents in the water sector, the range of options considered in their classification scheme and the limited number of cybersecurity incidents reviewed limits the ability to gain deeper insight into techniques, trends and patterns related to previous cybersecurity incidents (Hassanzadeh et al., 2020). Furthermore, their analysis does not correlate to international frameworks such as MITRE's ATT & CK for ICS.

Cybersecurity Incidents

In this section we review the cybersecurity incidents in the water sector and analyse their attack mechanism (adversarial behaviour) using the tactics and techniques of the MITRE & CK (Alexander et al., 2020; Mitre, 2022). Table provides the comprehensive cyber incidents in the water sector, and each incident contains a name, year of occurrence, confirmed/suspected threat actor, attack technique and type, targeted component/layer, and impact.

1. Maroochy Shire sewage incident

a. Summary of incident
   In March 2000, Maroochy Shire Council experienced problems with its new wastewater system (Slay and Miller 2008). Communications sent by radio links to wastewater pumping stations were being. Pumps did not work correctly, and alarms that were supposed to notify system engineers of faults did not activate as expected (Hemsley and Fisher 2018). Initially,

they thought the problem was due to the new system, but after some time, they noticed that the system was hacked. An engineer who was monitoring every signal passing through the system, discovered that someone was hacking into the system and deliberately causing the problems. The water utility hired a team of private investigators who located the attacker and alerted police. The attacker, Vitek Boden, was arrested and eventually jailed; he was an employee of a contractor that supplied IT/control system technology.

b. Attack mechanism

Mr. Boden used a laptop computer and a radio transmitter to take control of 150 sewage pumping stations (Slay and Miller 2008). Over a three-month period, he released one million liters of untreated sewage into a stormwater drain from where it flowed to local waterways. The attacker was physically located by the authorities and found in the possession of a laptop with a stolen software for SCADA reconfiguration installed, along with Motorola M120 two-way radio and PDS control devices. Evidence retrieved from the laptop also indicated that commands from the system program run at least 31 times, which matched the behavior observed in the company's logs (Makrakis et al., 2021). The attack was motivated by revenge on the part of Mr. Boden after he failed to secure a job with the Maroochy Shire Council.

The adversarial tactics and techniques used during this cyberattack are mapped using the MITRE ATT&CK framework in Table 3.1.

Table 3.1 Adversarial tactics and techniques used to conduct the Maroochy Shire sewage incident

Tactic	Technique (ID)
Initial access	Wireless Compromise (T0860)
Execution	
Persistence	
Privilege Escalation	
Defense evasion	
Credential Access	
Discovery	Remote system discovery (T088) T0808
Lateral Movement	Default credentials (T0812)
Collection	Automated collection (T0802)
Command and Control	
Inhibit Response Function	
Impair Process Control	
Impact	

2. Bowman Avenue dam incident

a. Summary of the incident

Iranian hackers gained unauthorized access to the SCADA systems of New York's Bowman Avenue Dam in 2013 which allowed them to gather information on water levels, temperature, and the status of the sluice gate (Shimon et al., 2015). The Bowman Dam controls storm surges, and Its SCADA system was connected to the Internet via a cellular modem (Hemsley and Fisher 2018).This access would allow the attacker to remotely operate and manipulate the dam's sluice gate. However, in this instance, the sluice gate had been manually disconnected for maintenance at the time of the attack**.**

b. Attack mechanism

The attackers exploited a vulnerability to identify an unprotected computer that controlled sluice gates and other functions of the dam. The attacker detected the vulnerability through "Google Dorking," a process of performing advance Google searches to detect vulnerabilities, and then implemented other technologies to successfully exploit the system (Germano, 2019).

The adversarial tactics and techniques used during this cyberattack are mapped using the MITRE ATT&CK framework in Table 3.2.

Table 3.2 Adversarial tactics and techniques used to conduct the Bowman Avenue dam incident

Tactic	Technique (ID)
Initial access	Internet accessible device (T0883)
Execution	
Persistence	
Privilege Escalation	
Defense evasion	
Credential Access	
Discovery	
Lateral Movement	
Collection	
Command and Control	
Inhibit Response Function	Activate Firmware update(T0800)
Impair Process Control	Brute force(T0806)
Impact	Damage to property (T0879)

3. Kemuri water company incident

a. Summary of the incident

Verizon Security Solutions reported that an undisclosed water company experienced a cyberattack on its ICSs by a suspected Syrian hacktivist group in 2016 (Andreeva et al. 2016; Hemsley and Fisher, 2018). Verizon gave a pseudonym of "Kemuri" to the water company (KWC) to protect its identity due to security reasons. The assessment took place after employees became suspicious of an intrusion due to irregular value and duct behavior (Makrakis et al. 2021). Attacker managed to manipulate the system to alter the amount of chemical entering the water supply and affect water treatment and production capabilities, causing water supply recovery times to increase (Hemsley and Fisher 2018).

b. Attack mechanism

KWC's plant had an old IBM AS/400-based SCADA system for managing the PLCs to regulate the flow of water and chemicals by managing valves and ducts in the plant. According to reports published by the security firm Vericlave (Vericlave, 2018) and other sources (Adepu et al., 2020; Alladi et al., 2020) the primary attack vectors used in the security breach of KWC's internal AS/40 system could have been a Structured Query Language (SQL) injection attack and email phishing. The attackers extracted login credentials for the system from the front-end web server to access the plant's water control software which was also running on the same AS/400 system. As this system was central to most IT operations in this plant, access to this control system allowed hackers to control most of the other equipment in the plant (Desc4). Although the attackers were able to manipulate the valves that control the chemical flow, there was no impact on the plant's operation. Personal information of about 2.5 million customers was also reported to have been leaked from their database (Alladi et al., 2020).

The adversarial tactics and techniques used during this cyberattack are mapped using the MITRE ATT&CK framework in Table 3.3.

Table 3.3 Adversarial tactics and techniques used to conduct the Kemuri water company incident

Tactic	Technique (ID)	Description
Initial access	-Exploit public facing application (T819) *-Phishing (T1566)*	-SQL injection on payment portal website, combined with spear-phishing for missing info
Execution		
Persistence		
Privilege Escalation		
Defense evasion	Exploitation for Evasion(T0820)	
Credential Access		
Discovery	*Remote system discovery (T0486)*	
Lateral Movement	-Valid Accounts (T0859)	- Webserver held files with plaintext credentials and IP of internal IBM AS/400 server
Collection		
Command and Control	Commonly used port (T0885)	
Inhibit Response Function	Activate firmware update (T0800)	
Impair Process Control	-Modify parameter (T0836)	-Attackers manipulated chemical flow twice, but alarms caused operators to intervene and prevent real impact (Modify parameter)
Impact	ATT&CK Enterprise (Exfiltration)	- Attackers exfiltrated 2.5 million customer data records

4. Israel water treatment incident

a. Summary of the incident

In April 2020, a cyber-attack targeted the industrial control systems of the Israel Water Authority's water treatment facility (Kovacs, 2020b). According to a statement from Israel's National Cyber Directorate, the attempted attack targeted the command-and-control systems of Water Authority's wastewater treatment plants, pumping stations, and sewage infrastructure (Kovacs, 2020a). Attacker gained access to water treatment systems and tried altering water chlorine levels. Israeli authorities issued an alert urging water treatment facilities affected by the attack to immediately reset the passwords and other ICS operators to consider additional security measures on their publicly accessible operational systems.

b. Attack mechanism

The adversarial tactics and techniques used during this cyberattack are mapped using the MITRE ATT&CK framework in Table 3.4.

Table 3.4 Adversarial tactics and techniques used to conduct the Israel water treatment incident

Tactic	Technique (ID)	Description
Initial access	-Internet Accessible Device (T883)	-Sites likely internet-connected using cellular gateways, rendering PLCs either directly or indirectly internet exposed
Execution		
Persistence		
Privilege Escalation		
Defense evasion		
Credential Access		
Discovery		
Lateral Movement	Default credentials (T0812)	- Reportedly no or default credentials on gateways and PLCs
Collection		
Command and Control	-Commonly Used Port (T0885) -Standard application layer protocols (T0869)	-Attacker communicated with PLCs using standard protocols on common ports (Siemens S7comm (102/TCP),Modbus TCP (502/TCP), GE SRTP (18245/TCP, 18246/TCP)
Inhibit Response Function		
Impair Process Control	-Modify Parameter (T836)	Attackers modified control logic and parameters
Impact	-Manipulation of control (T831)	-Attempted to increase chlorine levels

5. Florida water treatment incident

a. Summary of the incident

In February 2021, a unidentified cyber threat actors tried to manipulate Sodium Hydroxide (Lye) levels in the water treatment facility in Oldsmar town, Florida; USA (FBI 2021; Mass 2021). It has been publicly acknowledged that an operator machine had a remote access software package installed and accessible to the Internet. This led the attack to be carried out by gaining access to remote workstation using TeamViewer and manipulation of control set points for the dosing rate of Sodium Hydroxide (NaOH) into the water. *The attacker raised the NaOH does setpoint from its normal setting of 100 part-per-million (ppm) to*

11,100 ppm (Serino and Miller, 2021)**.** The operator quickly noticed the mouse cursor moving on his screen and changed the Sodium Hydroxide levels to normal operating parameters so that pH monitoring alarms did not detect a level beyond acceptable parameters.

b. Attack mechanism

The cyber actors likely accessed the system by exploiting cybersecurity weakness, including poor password security, and an outdated operating system. According to the joint FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) cybersecurity advisory (FBI 2021), it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system.

The adversarial tactics and techniques used during this cyberattack are mapped using the MITRE ATT&CK framework in Table 3.5.

Table 3.5 Adversarial tactics and techniques used to conduct the Florida water treatment incident

Tactic	Technique (ID)	Description
Initial access	-Exploit public-facing application (T0819) -External remote services (T0866)	
Execution	Execution through Graphical User Interface (T0823)	
Persistence	Valid accounts (T0859)	
Privilege Escalation		
Defense Evasion		
Credential Access		
Discovery		
Lateral Movement		
Collection		
Command and Control		
Inhibit Response Function		
Impair Process Control	-Modify parameter (T0836) -Unauthorized command message (T0855)	
Impact	-Loss of safety (T0880)	-Safety of lives drinking that water would have been lost
	-Manipulation of control (T0831)	-the chemical level control put in place was manipulated.

6. Summary of cybersecurity incidents in the water sector

Table 3.6 presents a summary of cybersecurity incidents in the water sector. The table highlighted the incident name, year, and county in which the attack was reported. It also lists the target component/layer (corporate network -CN, supervisory network -SN, local control network -LN, field or instrumentation network -FN), impact of the attack, the technique/method used to launch the attack, and vulnerable component.

Table 3.6 A summary of cybersecurity incidents in the water sector

Cyber Incident Name	Year	Attack location	Target	Threat actor	ATT & CK technique (initial compromise)	Attack type
Salt River Project	1994	United States	CN	Individual	Internet accessible device (T0883)	Malware(backdoor)
Maroochy Shire Sewage Spill	2000	Australia	SN	Individual	Wireless compromise (T0860)	Disgruntled Employee
Baseline Audit Uncovers Virus in Water Control System	2003	Australia	LN	Unknown		Virus
Trojan Backdoor on Water SCADA System	2004	Canada	SN	Unknown	*Spear phishing attachment (T0865)*	Malware (trojan backdoor)
Routine Audit of SCADA Laptop Identifies Virus	2005	Australia	CN	Unknown		Virus
Pennsylvania Water Company Hack	2006	United States	CN	Unknown	Internet accessible device (T0883)	malware
California Canal System Hack	2007	United States	SN	Individual (Insider)		Disgruntled employee
Wastewater Treatment District Hacked	2012	United States	CN	Individual (insider)		Disgruntled employee
Iranian cyberattack on New York dam	2013	United States	SN	Organized group	Internet accessible device (T0883)	Targeted attack
TGB water station hacks	2014	United States	CN	Individual (insider)		Disgruntled employee
European Public utility services attacked	2014					
Drinking water utility cellular	2016	United States	LN		Wireless compromise (T0860)	

routers hacked						
Suspicious network traffic data undisclosed location	2016	United States	LN			malware
“Kemuri” Water Company	2016	United States	SN	Organized group	Exploit public-facing application (T0819)	SQL injection and phishing
Clark County water hack	2016	United States				Ransomware
City of Atlanta ransomware attack	2018	United States	CN	Organized group/cybercriminals	-Drive-by-compromise (T0817) / Spearphishing attachment (T0865)	Ransomware
Crypto miner European water utility company	2018	Europe	SN		Drive-by compromise (T0817)	Cryptocurrency malware (Cryptojacking attacks)
Onslow Water and Sewer Authority	2018	United States	CN	Organized groups/cyber criminals		Ryuk Ransomware attack
Riviera Beach Water Utility ransomware	2019	United States	CN,LN , FN	Organized groups	Spearphishing attachment (T0865)	Ransomware attack
Israel’s water system facilities	2020	Israel	LN	Nation state		Targeted attack
Israel’s agricultural water pumps	2020	Israel				
Recycled water reservoir	2020	Israel				
Volue ASA Ransomware attack	2021	Norway	CN	Unknown	Spearphishing (T0865)	Ransomware attack
San Francisco Bay Area water treatment incident	2021	United States	LN	Unknown	Exploit public-facing application (T0819)	
Florida Water Treatment Plant	2021	United States	SN	Unknown	-Exploit public-facing application (T0819) -Exploitation of remote services (T0866)	

Analysis of Cyberattacks

This section provides an analysis of cybersecurity incidents from different perspectives (e.g., cyber threat actors, targets, techniques, impact, etc). Table shows the number of cybersecurity incidents and their attack techniques, targeted components, and impacts. Using our investigation of these cybersecurity incidents, we present the following key attributes, and their patterns and trends that be used for defence and threat intelligence in the water sector and other CIs.

1. Threat actors

Figure 3.1 represents the *threat actors* for the cybersecurity incidents reviewed in the previous section. When analysing trends from threat actors, it is also important to note the motivation behind these attacks. We found *i* individual (both internal and external), *j* organized groups, *k* nation state, *l* unknown threat actors. Many individuals carried out attacks due to personal reasons for either financial gain or as methods of retribution.

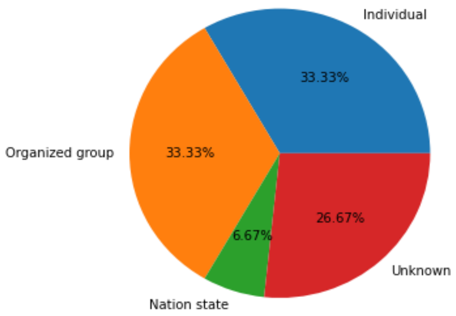


Figure 3.1 Threat actors

2. Initial access

The *initial access techniques* from the MITRE ATT&CK and ATT&CK ICS Frameworks is used when categorising the techniques identified from each cybersecurity incident within Section 5 (Mitre 2022a, 2022b). Figure 3.2 details the *attack techniques* used in the cybersecurity incidents in Table . 5 of the incident analyzed utilized an *internet accessible device*, y took advantage of a *wireless compromise*, z of the attacks involved *exploit public-facing application*, x incidents used *spear phishing*, and y others used *drive-by -compromise*.

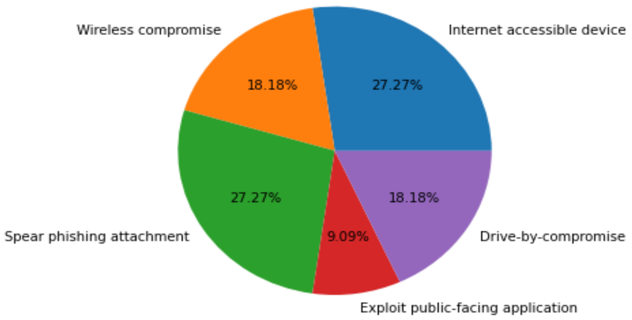


Figure 3.2 Initial access techniques

3. Target layers

Figure 3.3 depicts the distribution of cybersecurity incidents by the ICS target layer. X of water sector incidents targeted the corporate network layer, y the supervisory network, z the local control network, but k targeted the field device network.

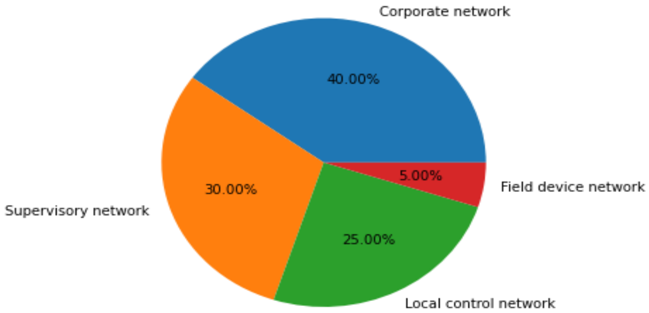


Figure 3.3 Target layers

Conclusions

Process surveillance and efficient control are essential for achieving the requirements in wastewater treatment. The digital tools that can be used in the water sector are numerous, but very useful are the software sensors that can be used in surveillance and control. The need for software sensors arises from the fact that physical sensors (e.g., for the organic load) are inexistent of very expensive.

Process surveillance and control are sufficient for obtaining a good quality of the effluent, but they do not protect the plant from cyber-attacks, and they must be coupled with cybersecurity procedures. It is thus important that the industry understands the risks and act accordingly. In addition, materials/classes on process surveillance, control and cybersecurity must be developed and used for training the wastewater treatment engineers.

References

Adepu, Sridhar, Venkata Reddy Palleti, Gyanendra Mishra, and Aditya Mathur. 2020. “Investigation of Cyber Attacks on a Water Distribution System.” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12418 LNCS(0): 274–91

Alex J, Benedetti L, Copp J, Gernaey K, Jeppsson U, Nopens I, Pons M, Rosen C, Steyer J, Vanrolleghem P (2008) Benchmark simulation model no. 2 (bsm2). Report by the IWA Taskgroup on benchmarking of control strategies for WWTPs pp 1–99.

Alexander, Otis, Misha Belisle, and Jacob Steele. 2020. “MITRE ATT&CK ® for Industrial Control Systems: Design and Philosophy.”

Alladi, Tejasvi, Vinay Chamola, and Sherali Zeadally. 2020. “Industrial Control Systems: Cyberattack Trends and Countermeasures.” Computer Communications 155: 1–8.

Andreeva, Oxana et al. 2016. “INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS.” https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word- (August 11, 2022)

Ariens, D., B. Houska, H. Ferreau, ACADO toolkit website. http://www.acadotoolkit.org.

Ariens, D., B. Houska, H. Ferreau, F. Logist, “ACADO for Matlab User’s Manual”, Optimization in Engineering Center (OPTEC), 1.0 beta edition, May 2010.

Barbu, M., I. Santin, and R. Vilanova, "Applying Control Actions for Water Line and Sludge Line to Increase Wastewater Treatment Plant Performance," Industrial and Engineering Chemistry Research, vol. 57, no. 16, pp. 5630-5638, 2018.

Bergmeir, C., R. J. Hyndman, and B. Koo, "A note on the validity of cross-validation for evaluating autoregressive time series prediction," Computational Statistics & Data Analysis, vol. 120, 2018.

Chen, C.T. “Linear System Theory and Design”, Philadelphia, PA, USA: Saunders College Publishing, 1984.

Cheung, Steven et al. 2006. “Using Model-Based Intrusion Detection for SCADA Networks” http://digitalbond.com (May 12, 2022)

Chi B, and L. Guo, "Wastewater treatment sensor fault detection using RBF neural network with set membership estimation," Chinese Control and Decision Conference (CCDC), Nanchang, China, pp. 2685-2690, 2019.

Christiansson, Henrik, and Eric Luiijf. 2008. “Creating a European SCADA Security Testbed.” IFIP International Federation for Information Processing 253: 237–47.

Council Directive 91/271/EEC of 21 May 1991 concerning urban waste-water treatment The Urban Waste Water Treatment Directive (UWWTD)

Dasarathy B., “Optimal control of nonlinear systems”, IEEE Transac- tions on Automatic Control, 15(6), 690?692, 1970.

DeCarlo, R. “Linear Systems: A State Variable Approach with Numer- ical Implementation”, Prentice Hall, NJ, 1989.

Drewnowski J, Szeląg B, Xie L, Lu X, Ganesapillai M, Deb CK, Szulżyk-Cieplak J, Łagód G. The Influence of COD Fraction Forms and Molecules Size on Hydrolysis Process Developed by Comparative OUR Studies in Activated Sludge Modelling. Molecules. 2020 Feb 19;25(4):929. doi: 10.3390/molecules25040929.

FBI, CISA,EPA, and MI-ISAC. 2021. “TLP: WHITE Compromise of U.S. Water Treatment Facility SUMMARY.” www.fbi.gov/contact-us/field-offices, (August 11, 2022)

Germano, Judith H. 2019. “Cybersecurity Risk & Responsibility in the Water Sector Prepared By.” : 6–19. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

Ghinea LM, Miron M, Ratnaweera H. A Deep Learning Approach for Faults Recognition of Dissolved Oxygen Sensor in Wastewater Treatment Plants. ETFA 2023

Goodfellow I., Y. Bengio, and A. Courville, "Deep Learning". MIT Press Cambridge, 2016, vol. 1.

Hassanzadeh, Amin et al. 2020. “A Review of Cybersecurity Incidents in the Water Sector.” Journal of Environmental Engineering 146(5): 03120003

Hemsley, Kevin E, and Ronald E Fisher. 2018. “History of Industrial Control System Cyber Incidents.” INL/CON-18-44411-Revision-2 (December): 1–37. https://www.osti.gov/servlets/purl/1505628

Housh, Mashor, and Ziv Ohar. 2018. “Model-Based Approach for Cyber-Physical Attack Detection in Water Distribution Systems.” Water Research 139: 132–43

Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams. 2006. “Security Issues in SCADA Networks.” Computers & Security 25(7): 498–506

Jacod J., P. Protter, “Discretization of Processes”, Springer, 2011.

Khalil H. K., “Nonlinear Systems”, Third Edition, Prentice hall Upper Saddle River, NJ, 2002.

Kovacs E. 2020a. “Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources | SecurityWeek.Com.” https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources (August 12, 2022).

———. 2020b. “Israel Says Hackers Targeted SCADA Systems at Water Facilities | SecurityWeek.Com.” https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities (August 12, 2022)

Liu Y., Y. Jiang, and I. Bortone, “A Scheme for Anaerobic Digestion Modelling and ADM1 Model Calibration”, Chemical Engineering Transactions, vol. 96, 2022.

Luenberger D.G., “Optimal Control. Introduction to Dynamic Systems”, New York: John Wiley & Sons, pp. 393?435, 1979.

Makrakis, Georgios Michail et al. 2021. “Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents.” IEEE Access 9: 165295–325

Mamandipoor B, M. Majd, S. Sheikhalishahi, C. Modena, and V. Osmani, "Monitoring and detecting faults in wastewater treatment plants using deep learning", Environ. Monit. Assess. vol. 192, issue 2, 2020.

Manamperuma, L., Wei, L., Ratnaweera, H. Multi-parameter based coagulant dosing control. Water Science and Technology 75 (9), 2017, 2157-2162

Mass, Massachusetts Department of Environmental Protection. 2021. “Cybersecurity Advisory for Public Water Suppliers | Mass.Gov.” https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers (August 11, 2022)

Miller, Bill, and Dale C. Rowe. 2012. “A Survey of SCADA and Critical Infrastructure Incidents.” RIIT’12 - Proceedings of the ACM Research in Information Technology: 51–56

Mitre. 2022. “ATT&CK® for Industrial Control Systems.” https://collaborate.mitre.org/attackics/index.php/Main_Page (August 8, 2022).

Moraitis, Georgios et al. 2020. “Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats.” Journal of Environmental Engineering 146(9): 04020108. https://ascelibrary.org/doi/abs/10.1061/%28ASCE%29EE.1943-7870.0001765 (May 11, 2022).

Naduvil-Vadukootu, R. A. Angryk, and P. Riley, "Evaluating pre-processing strategies for time series prediction using deep learning architectures," The Thirtieth International Flairs Conference, 2017.

Nair, A., Hykkerud, A., Ratnaweera, H. Estimating Phosphorus and COD Concentrations Using a Hybrid Soft Sensor: A Case Study in a Norwegian Municipal Wastewater Treatment Plant. Water 14 (3), 2022, 332

Necoara, I. “Model predictive control for hybrid systems: piecewise affine and maxplus-linear systems”, VDM, 2008.

Necoara, I. “Metode de optimizare numerica”,Editura Politehnica Press, Bucuresti, 2013.

Pisa I., A. Morell, R. Vilanova, and J. L. Vicario, "Transfer Learning in Wastewater Treatment Plant Control Design: From Conventional to Long Short-Term Memory-Based Controllers," Sensors, vol. 21, no. 18, p. 6315, Sep. 2021, doi: 10.3390/s21186315.

Pisa I., "Artificial Neural Networks in the Wastewater Industry From Conventional to Data-based Industrial Control", Ph.D. Thesis in Electronic and Telecommunication Engineering, Universitat Autonoma de Barcelona (UAB), Spain, 2022.

Ramotsoela, Daniel T., Gerhard P. Hancke, and Adnan M. Abu-Mahfouz. 2019. "Attack Detection in Water Distribution Systems Using Machine Learning." Human-centric Computing and Information Sciences 9(1): 1–22

Rasekh, Amin et al. 2016. "Smart Water Networks and Cyber Security." Journal of Water Resources Planning and Management 142(7): 01816004

Ratnaweera, H., Fettig, J. State of the Art of Online Monitoring and Control of the Coagulation Process. Water 2015; Volume 7.(11) p. 6574-6597.

Salles R., J. Mendes, R. P. Ribeiro, and J. Gama, "Fault Detection in Wastewater Treatment Plants: Application of Autoencoders Models with Streaming Data", section in book "Machine Learning and Principles and Practice of Knowledge Discovery in Databases", pp. 55- 70 2023.

Santin I., C. Pedret, R. Vilanova, and M. Meneses, "Advanced decision control system for effluent violations removal in wastewater treatment plants," Control Engineering Practice, vol. 49, no. 2, 2016

Serino G, Ben Miller. 2021. "Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack | Dragos." https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/ (August 11, 2022)

Sharmeen, Shaila et al. 2021. "An Advanced Boundary Protection Control for the Smart Water Network Using Semi Supervised and Deep Learning Approaches." IEEE Internet of Things Journal

Shimon Prokupecz, Tal Kopan and Sonia Moghe. 2015. "Official: Iranians Hacked into New York Dam - CNNPolitics." https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html (August 12, 2022)

Slay, Jill, and Michael Miller. 2008. "LESSONS LEARNED FROM THE MAROOCHY WATER BREACH."

Socha L., "Linearization Methods for Stochastic Dynamic Systems", Springer, 2007.

Statisitics Norway. https://www.ssb.no/en. Accessed 10.06.2023

Tawfik, A., El-Gohary, F., Temmink, H. Treatment of domestic wastewater in an up-flow anaerobic sludge blanket reactor followed by moving bed biofilm reactor. Bioprocess Biosyst Eng (2010) 33:267–276. DOI 10.1007/s00449-009-0321-1

Vericlave. 2018. "VericlaveTM-The Kemuri Water Company Hack." www.sentryo.com (August 11, 2022)