A Cyber-Secured Operation for Water-Energy Nexus

Pengfei Zhao, Chenghong Gu, Member, IEEE, Zhidong Cao, Da Xie, Member, IEEE, Fei Teng, Member, IEEE, Jianwei Li, Xinlei Chen, Chenye Wu, Dongmin Yu, Xu Xu, and Shuangqi Li

Abstract—The wide implementation of information and communication technologies (ICT) cause power system operations exposed to cyber-attacks. Meanwhile, the tendency of integrated multi energy vectors has worsened this issue with multiple energy coupled. This paper proposes a two-stage risk-averse mitigation strategy for water-energy systems (WESs), incorporating power, natural gas and water systems against false data injection attacks (FDIA) under water-energy nexus. The FDIA on individual subsystems is modelled through hampering false data integrity to the systems. An innovative two-stage risk-averse distributionally robust optimization (RA-DRO) is proposed to mitigate uneconomic operation and provides a coordinated optimal load shedding scheme for the nexus system security. A coherent risk measure, Conditional Value-at-Risk (CVaR) is incorporated into the RA-DRO to model risk. A Benders decomposition method is used to solve the original NP-hard RA-DRO problem. Case studies are demonstrated on a WES under water-energy nexus and results show that the effectiveness of the method to mitigate risks from potential FDIA and renewable uncertainties. This research provides WES operators an economic system operation tool by optimally coordinating energy infrastructures and implementing reasonable load shedding to enhance cybersecurity.

Index Terms—Distributionally robust optimization, false data injection attacks, integrated energy system, mitigation strategy, risk aversion, water-energy nexus.

NOMENCLATURE

The superscript ‘$\text{i}$' and ‘$\text{r}$' representing 'scheduled' and ‘regulated’ respectively are omitted in section C. The superscript ‘$\text{in}$’ and ‘$\text{ter}$’ representing initial and terminal nodes of power bus, gas and water nodes are also omitted in this section to save space.

A. Indices and sets

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t$, $T$</td>
<td>Index and set of time periods.</td>
</tr>
<tr>
<td>$b$, $B$</td>
<td>Index and set of power buses.</td>
</tr>
<tr>
<td>$n$, $N$</td>
<td>Index and set of gas nodes.</td>
</tr>
<tr>
<td>$w$, $W$</td>
<td>Index and set of water nodes.</td>
</tr>
<tr>
<td>$i_e$, $l_e$</td>
<td>Index and set of generators.</td>
</tr>
<tr>
<td>$g$, $g_e$</td>
<td>Index and set of gas wells.</td>
</tr>
<tr>
<td>$w$, $WR$</td>
<td>Index and set of water reservoirs.</td>
</tr>
<tr>
<td>$j$, $J$</td>
<td>Index and set of renewable energy sources (RES).</td>
</tr>
<tr>
<td>$g_t$, $GT$</td>
<td>Index and set of gas turbines.</td>
</tr>
<tr>
<td>$wp$, $WP$</td>
<td>Index and set of water pumps.</td>
</tr>
<tr>
<td>$l_e$, $l_e$</td>
<td>Index and set of power lines.</td>
</tr>
<tr>
<td>$l_g$, $l_g$</td>
<td>Index and set of gas pipelines.</td>
</tr>
<tr>
<td>$l_w$, $L_w$</td>
<td>Index and set of water pipelines without pumps.</td>
</tr>
</tbody>
</table>

B. Parameters

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l_{wp}$, $L_{wp}$</td>
<td>Index and set of water pipelines with pumps.</td>
</tr>
<tr>
<td>$k_e$, $K_e$</td>
<td>Index and set of power loads.</td>
</tr>
<tr>
<td>$k_g$, $K_g$</td>
<td>Index and set of gas loads.</td>
</tr>
<tr>
<td>$k_w$, $K_w$</td>
<td>Index and set of water loads.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_l$</td>
<td>Attack injection level for FDIA.</td>
</tr>
<tr>
<td>$R_{l_e}^+$, $R_{l_e}^-$, $R_{g_t}^+$, $R_{g_t}^-$</td>
<td>Maximum up and down reserve capacity of generators, the gas turbine and water pumps.</td>
</tr>
<tr>
<td>$R_{wp}^+$, $R_{wp}^-$</td>
<td>Resistance of power line $l_e$.</td>
</tr>
<tr>
<td>$f_{l_e, max}$, $f_{g_t, max}$, $f_{w_p, max}$</td>
<td>Demand of power, gas and water.</td>
</tr>
<tr>
<td>$P_{g_t, max}$, $P_{w_p, max}$</td>
<td>Maximum and minimum output of gas source $i_g$.</td>
</tr>
<tr>
<td>$G_{l_e, max}$, $G_{l_e, min}$</td>
<td>Maximum and minimum output of gas pipelines $l_g$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma_{l_e}$</td>
<td>Coefficient for Weymouth equation.</td>
</tr>
<tr>
<td>$f_{l_e, max}$</td>
<td>Maximum gas flow of line $l_e$.</td>
</tr>
<tr>
<td>$c_{gt}$</td>
<td>Conversion coefficient for gas turbines.</td>
</tr>
<tr>
<td>$\eta_e$</td>
<td>Electrical efficiency for electrolyser.</td>
</tr>
<tr>
<td>$h_{l_e, max}$, $h_{l_e, min}$</td>
<td>Maximum and minimum limits for head pressure of water node connected with or without water pump.</td>
</tr>
<tr>
<td>$a_{l_e}$, $b_{l_e}$</td>
<td>Water pump characteristic coefficients.</td>
</tr>
<tr>
<td>$\sigma_{k_{pg}}$</td>
<td>Water consumption coefficient of power-to-gas.</td>
</tr>
<tr>
<td>$P_{k_{pg}, max}$, $P_{k_{pg}, max}$</td>
<td>Maximum limits of power, gas and water load shedding.</td>
</tr>
<tr>
<td>$\lambda_{l_e}^a$, $\lambda_{l_e}^b$, $\lambda_{l_e}^c$</td>
<td>Cost coefficients of generator $i_g$.</td>
</tr>
<tr>
<td>$\lambda_{l_e}$</td>
<td>Cost coefficient for output of gas well $i_g$.</td>
</tr>
<tr>
<td>$\lambda_{wr}$</td>
<td>Cost coefficient of water purchase.</td>
</tr>
</tbody>
</table>
\[ \lambda_{te}, \lambda_{rg}, \lambda_{wp}, \lambda_{wp}. \]

Cost coefficient for up and down reserve of generators, gas turbines and water pumps.

\[ \lambda^{re}_{e}, \lambda^{re}_{g}, \lambda^{re}_{wp}. \]

Regulation cost coefficient of power purchase, generators, RES, gas wells and water reservoirs.

\[ r_{te}, t_{te}, r_{gt}, t_{gt}, r_{wp}, t_{wp}. \]

C. Variables

- Up and down reserve capacity of generators, the gas turbine and water pumps.
- Phase angle at initial and terminal buses.
- Output of gas wells.
- Power flow and gas flow.
- Pressure of gas node \( n \).
- Injected gas flow and output of gas turbine.
- Power consumed by the electrolyser.
- Gas flow of pipe with and without water pump.
- Water pump power consumption.
- Elevation of water node connected with and without pump.
- Head loss and gain of water node.
- Water flow of pipe with and without water pump.
- Load deviation due to FDIA.
- Load shedding of power, gas and water.
- Generation of renewable energy sources.

I. INTRODUCTION

Modern energy management systems (EMS) with the increasing dependence on emerging information and communication technologies (ICTs), have massively facilitated the high efficiency, reliability and security of the EMS [1]. Meanwhile, the increasingly aggressive cyber-attacks are also growing in numbers. As a typical arbitrary cyber-attack, false data injection attack (FDIA) can be manipulated by adversaries to integrate falsified data into real-time meter measurement and thus to affect and mislead the system operators with erroneous decisions on operation and control [2, 3].

Present research work of investigating FDIA on EMS can be categorized in terms of the perspective of attackers or system defenders. As for attack modelling from adversaries, a class of unobservable FDIA are designed assuming the attacker has the knowledge of system historical data [4]. A generalized framework for investigating the vulnerability of power system nonlinear state estimator to FDIA is analysed in [5]. Meanwhile, a robust detector model is proposed to check the measurement statistical consistency with the ensured detectability. From the perspective of system defenders, detection modelling and corresponding algorithms have been investigated widely. State estimation is of great significance in EMS, which provides reliable state estimates for system operators on economic dispatch and reliability analysis [6]. State estimation is implemented based on redundant measurements to filter out corrupted data. Nevertheless, some judiciously designed FDIA can be masked and hidden and eventually bypass the state estimation.

Therefore, mitigation strategy for EMS against FDIA is considered as the final barrier for defending power systems since conventional state estimation is still employed which fails to detect stealthy designed FDIA in real practice. The mitigation strategy for intra-interval operational security against FDIA is proposed in [7]. A dynamic analytical framework is designed for analysing the impacts considering system variability in the short dispatch interval. Paper [8] proposes the mitigation strategy for a unit commitment by using a tri-level optimization model and the original problem is transformed into a bi-level mixed-integer programming. The previous work of the authors proposes a risk and mitigation strategy for integrated electricity and gas systems under FDIA in a moment-based hierarchical two-stage framework [9]. In comparison, the improvements of this paper over [9] are three aspects: i) water-energy nexus has gained extensive research attention. There is widely investigation of FDIA on power systems. However, WESs also require a cyber-secured operation scheme against FDIA. Since WESSs are more vulnerable than power systems or IESs with higher interdependencies; ii) the proposed WES is linked closer via power-to-gas (P2Gs), gas turbines and water pumps than with only one gas turbine. The complex couplings and interconnections among power, gas and water systems desire a cyber-secured operation scheme; iii) a risk-averse DRO is adopted in this paper considering the risk of uneconomic operation cost caused by FDIA and renewable uncertainties. However, paper [9] lacks risk analysis. Compared with the existing risk mitigation strategy against FDIA, the advancement of this paper is summarized in TABLE I.

The interdependencies between coupled energy systems have been largely promoted due to the rapid demand increase of multiple energy and the development of energy conversion technologies. Through fully exploiting the interdependency of integrated energy systems (IES), existing literature regarding IES operation mainly focuses on several aspects: i) economic-based operation for minimizing operation cost or maximizing economic gain under normal conditions, ii) reliability-based operation considering risks from reliability issues and iii) resilience-based operation strategies against natural disasters. Paper [10] proposes an economic system operation for IES considering the relief of power and gas flow congestions. The distributed optimization outperforms than centralized optimization method with parallel data processing. A security-constrained unit commitment is designed in [11] for enhancing the operational reliability of IES considering possible \( N - k \) contingencies. A two-stage RO is applied and the problem is solved by a second-order cone-based Column & Constraint Generation (CCG) approach.
In recent studies, the novel distributionally robust optimization (DRO) is widely deployed to overcome the disadvantages of RO and SO. DRO employs partial distribution information instead of requiring the specific full knowledge of distributions [12, 13]. Meanwhile, it is a data-driven approach, which yields less-conservative solutions than RO. A combined optimization for integrated electricity and heat systems is proposed in [14] considering renewable and ambient temperature uncertainties, which are characterized by DRO. Paper [15] investigates the operation schemes for energy hub systems (EHSs) considering renewable uncertainty and multimodality information.

The uncertainties bring risks into economic operation. Intuitively, risks in the proposed WES operation model can lead to abnormal high operation cost. Risk-averse optimization considers a coherent trade-off between system economic performance and risk, which has been applied with SO on energy system operation [16, 17]. Paper [16] develops a risk-averse stochastic programming model for unit commitment considering renewable energy uncertainty. A conditional value-at-risk (CVaR) is incorporated to assess the risk from renewable energy uncertainty. In [17], a day-ahead operational planning model for a regional energy service provider with electricity price uncertainty is proposed. The CVaR criterion is employed to hedge against the uncertainty. This paper utilizes a risk-averse DRO model, which outperforms the existing risk-averse SO models with more practical distributional information availability.

Under the era of water-energy nexus, water systems have been given higher attention in the recent research works. Traditionally, water and power systems are modelled and operated separately. However, the two systems are actually mutually interdependent [18]. Around 80% of the power consumed in water systems is used for pumping and distributing water [19]. In power systems, surplus water resources significantly contribute to the generation and conversion in power systems. The joint optimization of power and water systems have been investigated in existing work, targeting at reducing operation cost and emissions. An optimal water-power usage operation scheme is in [20] considering the couplings in an integrated power and water system (IPWS). An alternating direction method of multipliers-based optimization is used. Paper [21] utilizes the water as an effective resource to manage renewable generators combined with demand-side management. Very recent work proposes a two-stage robust optimization (RO) model for multi energy systems [22]. Wind uncertainty is handled and the proposed model is solved by a CCG method.

In this paper, the proposed water-energy system (WES) incorporates power, gas and water systems. It realizes the comprehensive coordination between energy infrastructures of the three independent systems. The increasing penetration of conversion technologies strengthen the coupling and interactions between electricity, gas and water systems. The interdependency is enhanced, leading to both beneficial and adverse impacts for WES. As for the beneficial impacts, the relatively lower price of gas sources can provide more economic operation solutions for WES; the surplus generation in the original independent energy system can supply loads in other sub-energy systems based on upcoming energy conversions. However, the strong interdependency of WES is detrimental to system security, i.e., reliability issues, natural disasters and cyber-attacks. The failure on power, gas or water systems will inevitably propagate to other sub-systems. Accordingly, the uneconomic operation is caused not only because of the individual complexities in each sub-system, but also due to the tight interdependencies. The higher the interdependency in a WES, the more vulnerable the WES is.

This paper proposes a risk-averse mitigation strategy to alleviate the uneconomic operation of WES against potential FDIA considering renewable uncertainty. FDIA is assumed to target at load meter readings of power, gas and water systems. The two-stage framework consists of i) day-ahead operation scheme prior to the FDIA and forecasting of renewable uncertainty and ii) the implementation of real-time recourse actions based on the FDIA and realization of renewable uncertainty. Load shedding and scheduling operation are considered as the recourse actions to mitigate the impact from FDIA. The ambiguity set for capturing the FDIA and renewable uncertainty is constructed based on Kullback-Leibler (KL) divergence. The coherent risk measure, i.e., CVaR is used to balance the trade-off between risk and computational performance. The proposed two-stage risk-averse distributionally robust FDIA mitigation strategy for WES is denoted as TSRA-FMS for simplicity. Bender’s decomposition approach is adopted to solve the TSRA-FMS problem.

The major contributions of this paper are as follows:

1) This paper develops a mitigation strategy against FDIA for WES. The water-energy nexus achieves optimal energy coordination under normal conditions but is more vulnerable to cyber-attacks. The interdependencies between power, gas and water systems are analysed under different FDIA scenarios.

2) It utilizes a two-stage optimization framework.
incorporating both day-ahead system operation under normal conditions and real-time mitigation scheme against potential FDIA. To defend and mitigate the FDIA, capacity reserve from generations are scheduled in the first stage and load shedding is implemented in the second stage.

3) The model incorporates CVaR into DRO. This risk-averse mitigation method has the benefits of: i) it inherits the advantages of RO and SO based on limited uncertainty distribution information with weakened robustness, ii) compared with moment-based ambiguity set, the ambiguity set constructed by KL divergence can flexibly shape the candidate distributions of both FDIA and renewable uncertainty and thus it yields less-conservative solutions and iii) the trade-off between the optimization performance and risk is modelled based on the incorporation of CVaR.

The remaining paper is organized as follows: section II models three types of FDIA in power, gas and water systems. The problem formulation of TSRA-FMS is given in section III. In section IV, the methodology of KL divergence-based TSRA-FMS considering CVaR as the risk measure is proposed. The case studies are given in section V. Section VI concludes the paper.

II. ATTACK MODELLING

This paper considers three types of FDIA and the attack modelling is in this section. State estimation is used to provide accurate snapshot of power systems and detect FDIA based on available measurements. Nevertheless, a stealthy designed FDIA can be undetectable and bypass the state estimation. The FDIA considered in this paper is designed on corrupting load measurement. Equation (1) and (2) show the original expression of bus power injection and line flow. The incidence matrices of bus-generator and bus-load are represented by $K_P$ and $K_D$, respectively. The shift factor matrix can be obtained from the linearized DC flow equation, which is used to approximate the change of active power flow. The incremental matrices of $BP$ and $PL$ are given in (3) and (4) due to FDIA.

\[
BP = K_P \cdot G - K_D \cdot D 
\]

\[
PL = SF \cdot BP 
\]

\[
\Delta BP = K_P \cdot \Delta G - K_D \cdot \Delta D 
\]

\[
\Delta PL = SF \cdot \Delta BP 
\]

The following conditions should be satisfied for a successful FDIA:

Condition 1: $\Delta G = 0$. The attack on the measurement of output of generation is ignored since this type of attack can be easily detected and corrected.

Condition 2: Zero injection buses, i.e., buses without generators or loads connected, are not attackable.

Condition 3: Load measurements are attackable.

Condition 4: The load measurement eventually impacts on branch flow measurement.

The resulting formulation in (5) is obtained based on the above conditions:

\[
\Delta PL = -SF \cdot K_D \cdot \Delta D 
\]

As proposed in [23], the FDIA targeting on the load measurements increases and decreases some loads simultaneously. And the total load is remained unchanged. The attack deviation is limited with the attack injection level $AIL$ in (7).

\[
\sum \Delta D = 0 
\]

\[
-AIL D \leq \Delta D \leq AIL D
\]

Constraint (8) and (9) limit the original and attacked power flow before and after the FDIA. However, in practice, the line capacity is always sufficiently large in case of overloading issues.

\[
PL \leq PL \leq PL 
\]

\[
PL + SF \cdot KD \cdot \Delta D \leq PL \leq PL + SF \cdot KD \cdot \Delta D 
\]

In the real implementation, constraints (10) and (11) are used as the explicit expressions of (6) and (7).

\[
\sum \Delta P_{k,e,t} = 0 
\]

\[
-AIL_{k_g} P_{k,e,t} \leq \Delta P_{k,e,t} \leq AIL_{k_g} P_{k,e,t} 
\]

\[
-AIL_{k_w} P_{k,e,t} \leq \Delta P_{k,e,t} \leq AIL_{k_w} P_{k,e,t} 
\]

III. CYBER-SECURED MITIGATION SCHEME

The proposed two-stage cyber-secured mitigation scheme for the uneconomic operation of WES includes: i) day-ahead operation scheme prior to the FDIA and renewable uncertainty and ii) real-time corrective redispatch scheme and security measures under the potential FDIA and the realization of renewable uncertainty. This section proposes the objective function of the mitigation scheme and the associated constraints.

A. WES Structure

The proposed WES structure is shown in Fig. 1, including a modified IEEE 30-bus power system, a 20-node gas system and a 10-node water system. The power system contains 5 power generators and 3 RES generators. Two P2G facilities interconnect RES generators and gas nodes, which converts the excessive power energy to hydrogen gas. A gas turbine transfers gas from node 8 to bus 13. In the water system, there are 2 water reservoirs and 3 water pumps. Water pumps connected with nodes 1, 2 and 6 consume power form buses 29 and 30. The water electrolyser of P2Gs consume water, which are supplied from node 5. It is to be noted that the gas and water nodes are similar to the electrical buses in power systems. Nodes are the points that connect two or more gas pipelines, where a certain volume of gas is delivered or injected. A typical gas node can be connected with gas pipelines, natural gas sources, gas wells, gas storage systems, gas compressors and gas loads. In water networks, the water pipelines and nodes are similar to the power lines and buses in power networks, which are used to describe pipe connections and endings. Water nodes in a water network can represent water supplies, storage, pumps and loads.
Fig. 1. The structure of WES.

B. Objective Function

The overall objective is to mitigate the uneconomic operation, which is separated into a hierarchical day-ahead and real-time optimization under normal conditions and FDIA, respectively. The structure of the proposed cyber-secured mitigation scheme is given in Fig. 2. The objective function of day-ahead operation is given in (14), including the i) day-ahead generation cost of electricity generators, gas wells, ii) reserve cost of generators, gas turbines and water pumps and iii) water purchase cost from reservoirs. It is to be noted that the reserve capacity is prepared for countering impacts from FDIA and renewable uncertainty in the second stage.

\[
F_1 = \min_{i_c \in E, g \in G, t \in T} \sum_{i_c \in E, g \in G, t \in T} \lambda_{i_c}^p P_{i_c,t}^s + \lambda_{i_c}^r P_{i_c,t}^r + \lambda_{i_c}^w P_{i_c,t}^w \\
+ \lambda_{i_g}^s P_{i_g,t}^s + \lambda_{w_f}^s P_{w_f,t}^s + \lambda_{w_r}^s r^+_t \\
+ \lambda_{i_g}^r r^+_t \text{,} \quad \text{subject to}\ 
\]

The second-stage sub-objective (15) is implemented under the presence of FDIA and renewable uncertainty, which involves i) the adjutant decisions on dispatching generators, gas wells, RESs and water purchase and ii) minimum joint load shedding.

\[
F_2 = \min_{i_c \in E, g \in G, t \in T, K_r, K_e, K_r \in E, K_g \in G} \sum_{i_c \in E, g \in G, t \in T} + \lambda^g_j (a^g_j - \xi_{j,t}) \\
+ \lambda_{k_e}^e p_{k_e,t}^l + \lambda_{k_g}^e p_{k_g,t}^l + \lambda_{k_r}^e p_{k_r,t}^l \\
+ \lambda_{k_e}^s p_{k_e,t}^s + \lambda_{k_g}^s p_{k_g,t}^s + \lambda_{k_r}^s p_{k_r,t}^s
\]

C. Day-ahead operation

The day-ahead operation determines the power generation schedule of generators and the reserve dispatch of generators, gas turbines and water pumps. The day-ahead operation scheme (16)-(39) is based on the renewable forecast without considering the risks of FDIA. The reserve capacity of generators, gas turbines and water pumps are limited in (16) and (17).

Constraints (18) and (19) provide the limits of output of generators, gas turbines and power consumption of water pumps. The DC power flow after the linearization is shown in (20) and (21). The power balance constraint is given in (22). Equation (23) regulates the output of gas wells.

In the gas system, gas pressure is constrained in (24). In constraint (25), it shows that the pressure at initial nodes are always larger than the terminal nodes because the gas system considered in this paper is of radial topology. Weymouth gas flow equations are given in (26) and (27). Equation (28) is the constraint of the output of gas turbines. P2G enables to utilize the surplus renewable power generation and convert it to gas. Equation (29) shows the gas output via P2G [24]. The gas nodal balancing equation is given in (30).

Equations (31)-(39) are constraints of water system. The output of water reservoir is limited in (31). The water pressure limit is given in (32) for pipes with and without water tanks. Constraints (32)-(44) describes the hydraulic characteristics of water pipes with and without water pumps including head gain and loss. In (35), the pressure head gain of water pump is shown. The hydraulic characteristic of pipes without water pumps is given in (36) based on Darcy-Weisbach equation [25]. Equation (37) presents the power consumption of water pump. The water flow magnitude is limited in (38). And the mass balance constraint of water system is presented in (39).

\[
0 \leq r_{i,j,t}^+ \leq R_{i,j}^+ \text{,} \quad \text{subject to}\ 
\]

\[
0 \leq r_{i,j,t}^- \leq R_{i,j}^- \text{,} \quad \text{subject to}\ 
\]

\[
P_{i,j,t}^s \leq P_{i,j,max} \text{,} \quad \text{subject to}\ 
\]

\[
P_{i,j,min} \leq P_{i,j,t}^- \leq P_{i,j,min} \text{,} \quad \text{subject to}\ 
\]

\[
\begin{align*}
\chi_{i,e} f_{i,t}^s &= \left( \theta_{i,e}^+ - \theta_{i,e}^- \right) \\
-\chi_{i,e} f_{i,t}^s &\leq f_{i,e}^s \leq \chi_{i,e} f_{i,t}^s 
\end{align*}
\]
\[
\sum_{i \in E_t} P_{s,t} + \sum_{j \in J_t} \omega_{s,j,t} + \sum_{i \in E_t} f_{s,i,t} - \sum_{i \in E_t} f_{s,i,t} + P_{g,t} = \sum_{k \in K_t} P_{k,t} + \sum_{i \in E_t} f_{s,i,t} \leq \sum_{k \in K_t} P_{k,t} + \sum_{i \in E_t} f_{s,i,t} (22)
\]

The rest of the second-stage constraints are not listed due to space limitation. The constraints of the second stage are the same as the first-stage constraints when the superscript 's' is replaced by 're', which denotes the regulated decision variables.

IV. Methodology

The proposed TSRA-FMS is a two-stage DRO framework with minmax formulation in the second stage problem. The linear TSRA-MS is firstly represented by compact form for notation brevity. Then the KL divergence-based ambiguity set of DRO is constructed to capture the FDIA and renewable uncertainty. In section C, the expression of CVaR is given and incorporated in the original formulation of TSRA-FMS. Finally, the mathematical reformulation is made and the solution algorithm is proposed.

A. Formulation in Brevity

Matrices and vectors are used for notation brevity of the TSRA-FMS problem. The original objective function of TSRA-FMS is given in (46) without considering the risk measure.

\[
\min_{x \in X, \ p \in \Omega} c^x + \sup_{\xi \in \Xi} \mathbb{E}[Q(x, \xi)]
\]

(46)

The risk-averse DRO incorporates the risk measure in the second-stage problem, which is given in (47). The first term c'x is the first-stage objective. The second term (1-\alpha)\mathbb{E}_p[Q(x, \xi)] represents the weighted expected second-stage objective and the last term \alpha R(Q(x, \xi)) is the weighted risk measure. The weighting coefficient \alpha ranges between 0 and 1. Equation (50) degrades to risk-neutral DRO model when \alpha = 0.

\[
\min_{x \in X, \ p \in \Omega} c^x + \sup_{\xi \in \Xi} \left[ (1-\alpha)\mathbb{E}_p[Q(x, \xi)] + \alpha R(Q(x, \xi)) \right]
\]

(47)

s.t. Ax \leq b,

(48)

\(Q(x, \xi) = \min_y f(y)
\)

(49)

s.t. Ex + Fy + G\xi \leq h,

(50)

The first-stage constraints are represented by (48). Equations (49) and (50) represent the second-stage objective function and constraints, respectively, where the coefficient of (49) is denoted by f.

B. Constructing the Ambiguity Set

Based on the distance between probability distributions, the discrepancy-based ambiguity set can be modelled, where \eta is the divergence tolerance. In (51) and (52), p and \text{pr}_\Xi are the true and reference probability distribution, respectively. Equations (51) and (52) are the implicit and explicit descriptions of distribution distance.

\[
\text{Dis} = \{p \in D_\xi : \mathbb{D}_\xi(p \| p_{\text{ref}}) \leq \eta \}
\]

(51)

\[
\mathbb{D}_\xi(p \| p_{\text{ref}}) = \int f(\xi) \log \frac{p(\xi)}{p_{\text{ref}}(\xi)} \text{d}\xi
\]

(52)

Equation (54) shows the KL-divergence function of variable a.

\[
\varphi_{KL}(a) = a \log a - a + 1
\]

(53)

C. Risk-Averse DRO

CVaR refers to a risk assessment which quantifies the tail risk of investment [26]. CVaR is developed to mitigate the shortcomings of value at risk. CVaR is initially applied in finance industries, which is then extended to portfolio problems in other fields, such as power systems [27].

The probability of Q(x, \xi) is limited by the threshold \zeta. The coherent risk measure CVaR is convex and monotonic. The probability of Q(x, \xi) not larger than the threshold \zeta is shown as:
3i(x,ζ) := \int_{Q(x,ζ)} p(ζ) dζ  

Where \( \Psi \) is the cumulative distribution function of \( Q(x,ζ) \), which is a fundamental element of VaR and CVaR. Moreover, \( \Psi \) is continuous and nondecreasing with respect to \( ζ \). The definition of \( β \)-VaR and \( β \)-CVaR are shown as (55) and (56).

\[
VaR_β(Q(x,ζ)) = \min{ζ ∈ R : \Psi(ζ, x) ≥ β}  
\]

\[
CVaR_β(Q(x,ζ)) = \frac{1}{1 - β} \int_{Q(x,ζ)>\bar{β}} Q(x,ζ) p(ζ) dζ  
\]

Since \( Q(x,ζ) \) is continuously differentiable and convex, the below formula can be derived [26, 28].

\[
CVaR_β(Q(x,ζ)) = \min{ζ ∈ R \mid \frac{1}{1 - β} \int_{Q(x,ζ)>\bar{β}} Q(x,ζ) p(ζ) dζ}  
\]

Where function \( Q(x,ζ) - ζ \) is used to determine the larger value between \( Q(x,ζ) - ζ \) and 0.

\[
Q(x,ζ) - ζ = \begin{cases} 
Q(x,ζ) - ζ & (Q(x,ζ) - ζ > 0) \\
0 & (Q(x,ζ) - ζ ≤ 0)
\end{cases}  
\]

The original objective function of TSRA-FMS is reformulated as (59) with weighted CVaR. When substituting CVaR in (59) with (58), (59) can be derived.

\[
\min_{x ≥ 0} \left\{ c^T x + \max_{p∈D(\Delta P_{x,k})} \left(1 - aE_p(Q(x,ζ)) + aCVaR_β(Q(x,ζ)) \right) \right\}  
\]

\[
G(x,ζ) := (1 - a)Q(x,ζ) + \frac{a}{1 - β} \tilde{a}  
\]

\[
\text{s.t.} \quad Q(x,ζ) - \tilde{a} - ζ ≤ 0, \quad \tilde{a} ≥ 0  
\]

When the strong duality holds, (60) can be reformulated to (61) and then further equivalent to (62) [29].

\[
\min_{x ≥ 0} \left\{ c^T x + \max_{p∈D(\Delta P_{x,k})} \left(1 - aE_p(Q(x,ζ)) + aCVaR_β(Q(x,ζ)) \right) \right\}  
\]

\[
\min_{x ≥ 0} \left\{ c^T x + \alpha \tilde{a} + \max_{p∈D(\Delta P_{x,k})} \left(\sum_{k=1}^{m} \eta G_k(x,ζ) \right) \right\}  
\]

Lagrange function (63) can be used to handle the inner maximization problem with its dual formulation (64).

\[
\ell(p, τ, μ) = \sum_{i=1}^{n} p_i G_i(x,ζ) + \tau \left(1 - \sum_{i=1}^{n} p_i \right) + μ \left(\sum_{i=1}^{m} p_{ref,i} \eta_i \left(\frac{p_i}{p_{ref,i}}\right)\right)  
\]

\[
\text{max \quad} \ell(p, τ, μ) = \tau + μ \left(\sum_{i=1}^{m} p_{ref,i} \eta_i \left(\frac{p_i}{p_{ref,i}}\right)\right)  
\]

Based on the Slater’s condition [30], the (65) and (66) can be made when \( η \) is larger than 0:

\[
\max_{p∈D(\Delta P_{x,k})} \left(\sum_{i=1}^{m} p_i G_i(x,ζ) \right) = \min_{\ell ≥ 0} \ell(p, τ, μ)  
\]

\[
\min_{\ell ≥ 0} \ell(p, τ, μ) = \tau + μ \left(\sum_{i=1}^{m} p_{ref,i} \eta_i \left(\frac{p_i}{p_{ref,i}}\right)\right) - 1  
\]

The derivation in (67) can be obtained when substituting the inner maximization problem in (62) with (66).

\[
\min_{\ell ≥ 0} \left\{ c^T x + \alpha \tilde{a} + \tau + μ \left(\sum_{i=1}^{m} p_{ref,i} \eta_i \left(\frac{p_i}{p_{ref,i}}\right)\right) \right\}  
\]

\[
\text{s.t.} \quad x ∈ X, \quad Q(x,ζ) - \tilde{a} - ζ ≤ 0, \quad \tilde{a} ≥ 0, \quad G(x,ζ) := (1 - a)Q(x,ζ) + \frac{a}{1 - β} \tilde{a}  
\]

Nevertheless, equation (67) is a nonlinear problem which requires to be linearized before the decomposition algorithm. For a given \( x = x^k \), when \( Q(x^k,ζ) < \infty \), \( Q(x^k,ζ) \) is subdifferentiable [31] and (68) can be obtained, where

\[
Dual(x^k) = \text{argmax} \{\pi' (h - Ex^k) : F'π ≤ f\}  
\]
increases $637428 from case 9 to 10. Consequently, it can be concluded that the increase rate of operation cost is highly affected by the AIL.

B. Studies on Load Shedding

Load shedding in three sub-systems is implemented to ensure the overall system security and maintain the feasibility of the proposed mitigation scheme. The optimal coordinated load shedding strategy considers power load shedding (PLS), gas load shedding (GLS) and water load shedding (WLS) for 24 hours under different levels of FDIA. Figs. 6-9 present the load shedding under different combinations of FDIA. In Fig. 6, it can be seen that PLS is affected by both P-FDIA and G-FDIA. PLS is not sensitive when the AIL of P-FDIA is below 8%. When G-FDIA is at 0%, PLS rises from 0MWh to 691MWh; when G-FDIA is at 20%, PLS rises from 0MWh to 1274MWh. Fig. 7 shows the GLS under P-FDIA and G-FDIA. The highest GLS, 589kcf, is obtained when the two types of FDIA are at the highest level. When solely conducting G-FDIA, GLS ranges between 400kcf and 589kcf. The PLS under P-FDIA and W-FDIA is shown in Fig. 8. The highest PLS (1990MWh) is implemented at 20% of AIL of P-FDIA and W-FDIA, which indicates the higher impact caused by W-FDIA compared with G-FDIA in Fig. 6. At the highest level of P-FDIA, increasing W-FDIA causes PLS growth from 709MWh to 1990MWh. Fig. 9 depicts WLS under P-FDIA and W-FDIA. The highest WLS is 257m$^3$ at the highest level of P-FDIA and W-FDIA.

<table>
<thead>
<tr>
<th>Node No.</th>
<th>$P_{w,r,\text{max}}$ (m$^3$/h)</th>
<th>$\lambda_{w,r}$ ($$/m^3$$)</th>
<th>Elevation (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>325</td>
<td>6.4</td>
<td>-252.5</td>
</tr>
<tr>
<td>2</td>
<td>700</td>
<td>2.6</td>
<td>-255</td>
</tr>
</tbody>
</table>

Table II: Parameters of Water Reservoirs
TABLE III
CASE ILLUSTRATION

<table>
<thead>
<tr>
<th>Case No.</th>
<th>Optimization method</th>
<th>P-FDIA</th>
<th>G-FDIA</th>
<th>W-FDIA</th>
<th>Renewable Uncertainty</th>
<th>AIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deterministic</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>RO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>5%</td>
</tr>
<tr>
<td>3</td>
<td>RO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>5%</td>
</tr>
<tr>
<td>4</td>
<td>DRO</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>5%</td>
</tr>
<tr>
<td>5</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>5%</td>
</tr>
<tr>
<td>6</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>5%</td>
</tr>
<tr>
<td>7</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>5%</td>
</tr>
<tr>
<td>8</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>10%</td>
</tr>
<tr>
<td>9</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>15%</td>
</tr>
<tr>
<td>10</td>
<td>DRO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>20%</td>
</tr>
</tbody>
</table>

TABLE IV
ECONOMIC PERFORMANCE FOR CASE 1-10

<table>
<thead>
<tr>
<th>Economic result</th>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
<th>Case 4</th>
<th>Case 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-stage cost ($)</td>
<td>843986</td>
<td>1031728</td>
<td>1037751</td>
<td>729817</td>
<td>748581</td>
</tr>
<tr>
<td>Expected Second-stage cost ($)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>125279</td>
<td>133381</td>
</tr>
<tr>
<td>Total cost ($)</td>
<td>843986</td>
<td>1031728</td>
<td>1037751</td>
<td>855096</td>
<td>881962</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Economic result</th>
<th>Case 6</th>
<th>Case 7</th>
<th>Case 8</th>
<th>Case 9</th>
<th>Case 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-stage cost ($)</td>
<td>759284</td>
<td>759910</td>
<td>804595</td>
<td>843697</td>
<td>889062</td>
</tr>
<tr>
<td>Expected Second-stage cost ($)</td>
<td>247276</td>
<td>248762</td>
<td>516593</td>
<td>994951</td>
<td>1632379</td>
</tr>
<tr>
<td>Total cost ($)</td>
<td>1008672</td>
<td>1008672</td>
<td>1321188</td>
<td>1838648</td>
<td>2521441</td>
</tr>
</tbody>
</table>

Compared with other FDIA scenarios, WLS increases smoothly when P-FDIA is at the highest level.

C. Scalability Analysis

In this section, the proposed TSRA-FMS is tested in a larger system scale to validate the applicability. This WES contains an IEEE 118-bus system, a 20-node gas system and a 10-node water system according to [32] and [33]. There are 54 power generators and 3 RES generators in the power system. RES generators are connected with buses 36, 69 and 77 with a capacity of 250MW. This analysis is conducted among 8 cases to demonstrate i) the effectiveness of TSRA-FMS on IESs, ii) comparison between risk-averse DRO and risk-neutral DRO and iii) the impact of system interdependency on system vulnerability. The case illustration is shown in TABLE V. Note that ‘system interdependencies’ indicates the number of connected gas and water systems in the WES. For instance, in case 1, the WES contains 3 gas systems and 3 water systems.

In Figs. 10 and 11, the water load shedding under cases 4 and 5 is given. Cases 4 and 5 are used to compare the proposed risk-averse DRO and risk-neutral DRO of [9]. In Fig. 11, the WLS reaches up to 983m$^3$ when P-FDIA and W-FDIA are both under 20% of AIL. When P-FDIA is not considered, the highest AIL of W-FDIA causes 77 m$^3$ WLS. Compared with Fig. 10, the risk-averse DRO presents a higher WLS than that of risk-neutral DRO, i.e., the WLS is 1168 m$^3$ under 20% of P-FDIA and W-FDIA, which is 19% higher than that of risk-neutral DRO.
5% of AIL is considered for Figs. 12 and 13. In Fig. 12, the second-stage expected cost under different sample size is given, where the black and blue curves represent cases 4 and 5, respectively. Overall, case 4 without considering CVaR shows lower second-stage expected operation cost under FDIA and renewable uncertainty. When 5000 second-stage samples are considered, the results of cases 4 and 5 approximates to $736000 and $80000. However, the result fluctuates when the data sample is below 500. In Fig. 13, the results show that the PLS in WES is higher than that in IES. For instance, cases 3 and 7 yield $567000 and $648000 PLS cost, respectively. Since W-FDIA causes WLS and the water reservoirs and pumps require higher usage. Accordingly, higher power consumption of water pumps leads to higher PLS. For case 5, there are 2 gas systems and 2 water systems, which shows $47000 higher cost than that of case 6 with 1 gas system and 1 water system. The additional 2 P2G facilities and 3 water pumps thus result in higher power consumption.

VI. CONCLUSION

Under the water-energy nexus era, the three proposed sub-systems are highly interwined. The cyber-attacks on any sub-system could propagate to the other two subsystems. Consequently, this paper proposes a two-stage risk-based mitigation strategy for the novel WES under water-energy nexus. Both the day-ahead and real-time operation schemes are determined with FDIA on three sub-systems. The FDIA and renewable uncertainty are captured via the proposed RA-DRO. The trade-off between the economic performance and risk caused by cyber-attacks and renewable fluctuation is provided. This two-stage mitigation framework with flexible risk alternative is solved by a tractable Bender’s decomposition method. Through the extensive studies, the key findings are listed below:

- Considering all types of FDIA, i.e., P-FDIA, G-FDIA and W-FDIA, leads to higher system economic loss than considering two types or one type of FDIA.
- PLS is more sensitive to W-FDIA compared with G-FDIA.
- The proposed RA-DRO mitigates the conservatism of RO with less load shedding.

The economic efficiency and system security under water-energy nexus is achieved via the effective proposed TSRA-FMS with optimally coordinated load shedding schemes to protect the entire system. The end energy users will benefit from this better supply security. This work is especially practical under smart cities with enormous water-energy interdependencies.

REFERENCES
