Toward a Cyber-Physical Digital Twin for Operator Training: Real-Time Co-Simulation of the French Grid

Frédéric Sabot*, Sami Ben Mariem*, Gautier Dekeyne*, Laurine Duchesne*, Alireza Bahmanyar*
Damien Ernst†, Olivier Bretteville‡, Thibaut Vermeulen‡, David Herve‡, Lucas Saludjian‡ and Geethu Joseph§
* Haulogy, Neupré, Belgium
† Montefiore Institute, University of Liège, Liège, Belgium
‡ R&D department, RTE Réseau de Transport d'Electricité, Paris, France
§ Cresym, Brussels, Belgium

***Abstract*—Modern power systems face an increasing need for operator preparedness against complex cyber-physical contingencies that may compromise grid stability. This paper presents a novel real-time co-simulation platform designed to serve as a digital twin of cyber-physical power systems. The platform has been used to simulate the entire French transmission grid in real-time with node-breaker topology while accounting for cyber contingencies in its SCADA infrastructure. The key to the platform's scalability is the use of an information flow modeling framework instead of cyber simulation detailed at the protocol level. In this framework, users model delays, drops, and data corruptions using stochastic processes. This abstraction covers not only communication impairments, such as delays or packet loss, but also computational slowdowns, database query latencies, and other cyber processes relevant to power system operation.**

***Index Terms*—Cyber-physical systems, digital twin, operator training, real-time co-simulation, SCADA interface, information flow model.**

I. Introduction

The reliable operation of large-scale transmission systems increasingly depends on the tight coupling between physical grid dynamics and their supporting cyber infrastructure. Supervisory Control and Data Acquisition (SCADA) systems, inter-control center protocols such as ICCP, and substation automation platforms based on IEC 61850 collectively form the backbone of this cyber layer, enabling wide-area monitoring, real-time control, and protective actions across geographically distributed assets. This integration, while enabling advanced functionalities, has given rise to complex cyber-physical power systems (CPPS), where disturbances originating in either domain can propagate and compromise system stability [1]. The large-scale blackout that struck the Iberian Peninsula in April 2025 exemplified how a complex chain of cyber-physical interactions—linking inadequate voltage control responses, protection relay actions, and interconnection tripping—can cascade into continent-scale consequences. On the top of these complex cyber-physical interactions, rises the growing threat of coordinated cyber-physical attacks, where malicious actors aim to exploit the tight coupling between communication networks and physical grid operations to disable protection schemes, distort measurement data, or delay control actions in ways that jeopardize system stability [2], [3].

Preparing operators to anticipate and respond to such contingencies requires analytical and training environments that represent both domains in a unified way. Co-simulation has emerged as a prominent approach to this problem: by coupling dedicated power system simulators with cyber-asset simulators, it becomes possible to capture the interdependencies between both worlds. Existing works have demonstrated the value of co-simulation for studying the effects of communication delays, packet loss, or malicious data injections on wide-area control and protection [4], [5]. Yet, conventional frameworks often struggle to balance fidelity and scalability: detailed protocol-level models are computationally prohibitive for national-scale studies, while highly abstracted models fail to provide the realism needed for operator preparedness.

To address these critical gaps, this paper presents a real-time cyber-physical digital twin of the French transmission grid at node-breaker granularity, achieved by integrating four key components: **(1)** an event-driven orchestrator that synchronizes cyber and physical dynamics in real time; **(2)** a modular and extensible implementation of the information-flow model [6], [7], where cyber elements and contingencies are modeled as stochastic processes; **(3)** the Dynaωo [8] power system simulator as the backbone for high-fidelity modeling of grid dynamics; and **(4)** a modular interface that can be used to interact with the orchestrator by consuming and producing data in the form of telemetry and control signals. This interface allows for the integration of SCADA-based human-machine interfaces (HMIs) for operators ("trainees"), HMIs for the "game master" or "trainer", and the integration of replica automata for hardware-in-the-loop style testing.

A key enabler of this national-scale real-time cyber-physical simulation is the use of an information flow model instead of a detailed cyber simulator (such as ns-3 or OPNET). Such approach takes the physical grid as the primary system of

interest and represents the cyber system exclusively through its impact on physical behavior.

Information flow modeling [6], [7] considers that cyber contingencies mainly affect the operation of the physical grid by affecting end-to-end information flows, i.e. by delaying, dropping, or distorting the data transmitted throughout cyber systems. It thus directly models those delays, drops, and data distortions using mathematical functions instead of modeling individual cyber elements down to the protocol level.

On top of scalability, a major advantage of information flow modeling compared to detailed simulation is its lower barrier to entry and higher control over the fidelity-scalability balance. Indeed, one could start with a very simple information flow model where all communication channels are represented with constant delays, and progressively introduce more complex models depending on the focus of the study and on data availability. A contrario, when performing detailed simulations, one needs to have models of all cyber elements, all implemented protocols (including legacy and proprietary ones), etc., information which might be very difficult or even impossible to obtain, especially when part of the cyber network is not directly owned by the TSO but rented by internet service providers through service level agreements.

Our information flow model implementation has been designed to be easily extensible and include not only simple mathematical models, but also more complex stochastic processes. For instance, channel availability may be captured by a two-state Markov process, while data integrity can be modeled through multi-level stochastic descriptions distinguishing credible from non-credible corruption or loss. These models can be flexibly instantiated within the framework or even trained from empirical measurements of real communication infrastructures. All such abstractions are synchronized with power system dynamics through the event-driven orchestrator, ensuring that cyber contingencies alter in real time the content of telemetry and control signals computed by Dynaωo.

To the best of the authors' knowledge, this is the first time real-time cyber-physical simulations have successfully been performed on a national-scale grid (with more than 6000 substations and 500k signals emitted per second). The developed platform will be made available open-source.

II. Platform Architecture

A. System Overview

The platform is designed around an orchestrator-centric architecture as shown in Fig. 1. The orchestrator coordinates four main elements: **(1)** the time-based power system simulation with **(2)** the cyber layer as modeled by the information flow model, **(3)** the operator training interface and **(4)** the Game Master interface through which the supervisor can inject disturbances and control the system. The physical dynamics of the transmission system are simulated with Dynaωo allowing scalable real-time node-breaker level simulation. The cyber layer is modeled using the information flow model. Its implementation allows modifying measurements and control signals by adding delay, altering values, or dropping them. The operator interacts with the system through a SCADA interface that reproduces the control room view.

B. Event-Based Orchestrator

The orchestrator provides the temporal backbone of the platform. It coordinates the different modules of the platform by treating all interactions as timestamped events. Events are stored in a priority queue ordered by execution time and are processed in chronological order. Modules can interact with each others through the orchestrator through a broker-based approach: each module emits events describing its outputs and subscribes to the events it needs to consume.

When a signal is generated, such as a measurement or a control command, it is placed in the event queue. The information flow model then processes this signal and applies the stochastic transformations that represent the selected cyber contingency. The modified signal is re-inserted into the queue and eventually delivered to its destination. In this way, delays, losses, or data changes introduced in the cyber layer are reflected in the power system response.

The orchestrator also supports logging, replay, and scenario control. All events are recorded with timestamps, allowing scenarios to be replayed and operator responses to be analyzed. The Game Master can inject or alter events to create disturbances and guide training exercises.

C. Power System Simulation

The power system simulation module provides the physical layer of the co-simulation platform. Its role is to compute the electrical state of the network and to generate/consume events that represent measurements and, control actions. Any simulator capable of providing state vectors at discrete time steps can in principle be integrated into the architecture, as long as it exposes its results to the orchestrator through a publish/subscribe interface.

In this work, we mainly use DynaWaltz, a simulator from the Dynaωo suite, developed at RTE, the French transmission system operator. DynaWaltz is designed for long-term stability studies. It models electrical phenomena on timescales from one second to several hours. Still, the platform remains compatible with other Dynaωo modules. In particular, the DynaSwing RMS simulator (modeling timescales in the order of 20ms to dozens of seconds) has been tested on small and medium networks. In the near future, it might also be possible to use it for real-time simulations of the French network provided the solver performance is improved, for example through multi-threaded implementations.

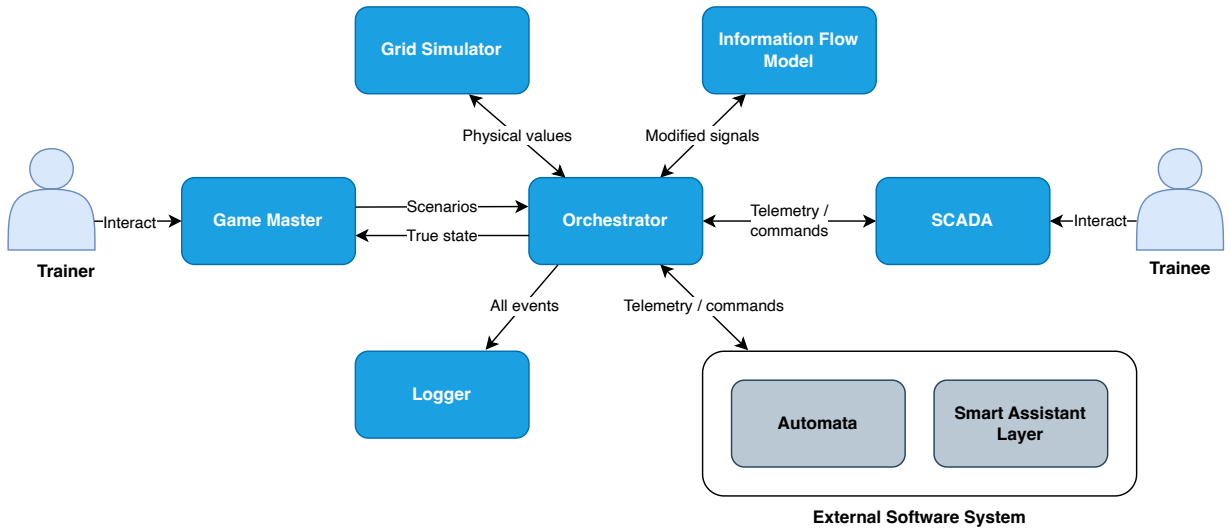

Fig. 1. Orchestrator-centric architecture coordinating the simulation components through a time-based event queue.

D. Cyber Layer Modeling

The cyber-contingency simulation module represents how information circulating between devices such as IEDs, RTUs, and SCADA servers can be impacted by cyber phenomena. Its role is to model the impact of cyber phenomena on telemetry and control signals, so that these effects can be propagated consistently to the power system simulation. Typical phenomena include additional transmission delay, message loss, and corruption of data.

In this work, these effects are modeled through an information flow model (IFM). The IFM abstracts the cyber layer as a directed graph where vertices represent devices and edges represent communication channels. Each signal produced by the power system simulator or by the trainee interface is treated as an event that traverses this graph. During this traversal, stochastic processes are applied to reflect the contingency under study. Depending on the configuration, a signal may be delayed, modified, or dropped before reaching its destination.

The stochastic processes used in the IFM are designed to be lightweight and composable, so that outcomes can be evaluated quickly even when the network of processes is deep. For instance, transmission delay can be modeled as an additive random variable drawn from a specified distribution, while packet loss can be represented by a Bernoulli trial with time-varying probability. Two-state Markov chains can capture bursty behavior or intermittent availability. This structure ensures that the framework remains scalable to national-scale grids with hundreds of thousands of concurrent signals.

In addition, the modular design allows the integration of high-fidelity models trained on real data in selected areas of interest. For example, data-driven models can be substituted for specific links or devices to reproduce empirical patterns of latency, loss, or corruption more accurately. This combination of lightweight stochastic abstractions for most of the system and detailed models for critical subsystems preserves scalability and ease-of-use while providing realism where it matters most.

E. Orchestrator Interface

A generic interface has been defined to connect external modules to the orchestrator. Through this interface, modules can publish and consume events in the same way as the power system simulator or the information flow model. This design makes the architecture extensible: any new training or supervision component can be added without changing the core of the orchestrator.

Three modules have been implemented using this interface. The first is the trainee interface, which reproduces the operational environment of French transmission control centers. It mainly provides a SCADA-compatible human-machine interface for operator training.

The second module is the Game Master interface, which provides oversight and scenario control. It gives supervisors a real-time view of the physical grid state, the trainee-perceived state, and the cyber infrastructure state. It allows disturbances to be injected, parameters to be modified dynamically, and trainee actions to be monitored. Training sessions can be coordinated, and operator performance can be evaluated with the help of logged events and replay functionalities.

The third module is an interface for external automata. This SCADA-compatible interface can be used for operator training and to test replica automata before implementing them in the field.

III. Results

This section presents the results obtained using our cyber-physical simulator, demonstrating its capability to test external

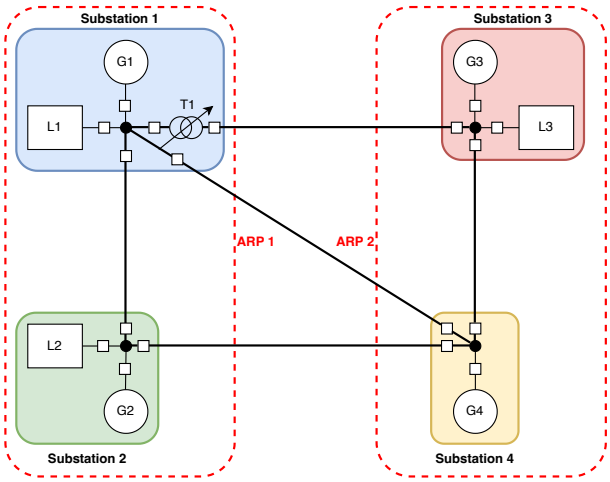

Fig. 2. Node-breaker view of the 4-bus test system.

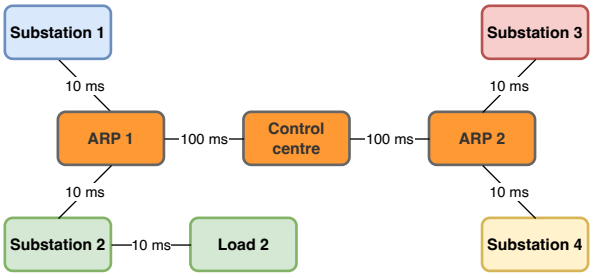

Fig. 3. Cyber view of the 4-bus test system. ARPs are aggregators connecting to multiple substations.

automata, to support operator training and to simulate the complete French transmission grid in real-time.

A. Test case 1: Automata testing in a 4-bus network

The first test case demonstrates the testing of a demand response automaton for an industrial consumer in a simple 4-bus system. The physical view of the 4-bus system is shown in Fig. 2 and its cyber view is shown in Fig. 3. The 4-bus system consists of 3 loads supplied by 4 generators. It has a peak load of 300MW, 150 of which are for the industrial load connected to the substation 2. In this test case, a demand response automata is proposed for the industrial load at substation 2 in order to help with frequency control.

The pseudocode of the demand response automaton is given in Algorithm 1. The automaton is designed to reduce the power consumption of the industrial load (by disconnecting processes that are interruptible) when the frequency falls below 49.5Hz (before standard under-frequency load shedding schemes act). Also, when the frequency falls outside the [48, 52Hz] range, it completely disconnects the load to protect sensitive assets. Frequency measurements are taken inside substation 2 and sent to load 2 where the automaton is located. For the sake of simplicity, a constant delay of 10ms is assumed between

Algorithm 1 Pseudocode of the industrial load control

```
if f < 48Hz or f > 52Hz then
    Disconnect load
else if f < 49.5Hz then
    Decrease load by 35MW
end if
```

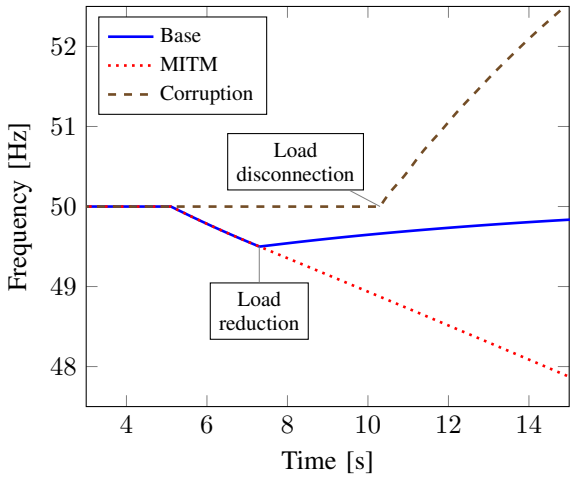

Fig. 4. Frequency evolution in the base, man-in-the-middle (MITM) and corruption scenarios.

substation 2 and load 2. Also, neither drops nor corruptions are considered in the base scenario.

Fig. 4 shows the evolution of the frequency following the disconnection of generator 2 (50MW capacity) at t=5s. As expected, the demand response automaton activates when the frequency falls below 49.5Hz which helps to stabilize the frequency. The results shown in this Figure have been obtained using Dynaωo with a synchronization time step of 100ms, i.e. Dynaωo is synchronized with the orchestrator every 100ms. It is worth to study the impact of this synchronization time step by looking at the timeline below:

- At t=7.2s, Dynaωo publishes a frequency of 49.49Hz (first time a frequency below 49.5Hz is reached).
- At t=7.2s, the orchestrator receives the frequency measurement from Dynaωo and forwards it to the information flow model.
- At t=7.2s, the information flow model evaluates the possible delays, drops and corruptions that will be applied to the frequency measurement between substation 2 and load 2. In this case, only a 10ms delay is added, so the reception of the frequency measurement is scheduled for t=7.21s and put in the event queue.
- At t=7.21s, the frequency measurement is popped from the event queue and sent to the demand response automata.
- At t=7.21s, the demand response automata activates and ask the orchestrator to forward the demand reduction to Dynaωo

- At t=7.3s, the orchestrator and Dynaωo are synchronized, and the demand reduction is actually implemented.

The above timeline shows that information going to/from Dynaωo might be delayed by up to one synchronization time step. This is a natural consequence of using a simulator with a fixed synchronization time step. Circumventing this limitation would require implementing additional features in Dynaωo such as roll back capabilities which might not be compatible with real-time simulation of large systems [4]. Instead, we chose to keep a constant synchronization time step and to make it sufficiently small to not significantly impact the simulation results. For the main objective of this work, which is operator training on the full French network, a synchronization time step of 1s has been judged sufficient as other delays overshadow it (e.g., SCADA interface and measurements are only updated every few seconds).

Fig. 4 also shows the results of two other scenarios on the 4-bus test system. The first one studies the impact of a man-in-the-middle (MITM) attack between substation 2 and load 2. In this scenario, the attacker intercepts frequency measurements and replace them with fake measurements of 50Hz to hide the frequency collapse from the demand response automaton. In the information flow model, this is modeled by adding a data corruption function that replace the value of all frequency measurements to 50Hz in the link between substation 2 and load 2. Fig. 4 shows that in this scenario the automaton does not act and the frequency collapses.

The last scenario considers possible data corruption in the channel between substation 2 and load 2. In the information flow model, this is modeled by a corruption function that has a small chance to replace the frequency measurement with a random float (i.e. non-credible data corruption).[1] In this scenario, we do not consider the initial generator disconnection, so the system is initially in steady-state. At t=10.21s, the automaton receives a corrupted frequency measurement with a value of -6.6e+37Hz and thus disconnects the load as it does not perform the necessary sanity checks on the received frequency measurement. This leads to a large frequency increase and system collapse due to the large size of the load compared to the size of the system.

B. Test case 2: Operator training on French network

The second test case is an operator training scenario simulated on the entire French network. In this scenario, two transformers are lost in the MQIS substation (shown in Fig. 5) due to internal faults. This leads to an overload in a third transformer in the substation. The trainee is made aware of this overload through an alarm in the SCADA interface and is made aware that he has 20 minutes to relieve the overload before the transformer is automatically tripped by its protection.

[1]Note that even if we did not explicitly model the cyber system at a granularity below the substation, such corruption function could be used to model data corruptions not only in the communication channel between substation 2 and load 2, but also anywhere else in the data acquisition chain.

Algorithm 2 Definition of the scenario using the DSL

```
1: set simulation duration to 30 minutes;
2: set time step to 1 second;
3: at 5 seconds, open switch "MQIS P7_MQIS 7AT762 DJ_OC";
4: at 15 seconds, open switch "MQIS P7_MQIS 7AT764 DJ_OC";
```

Figs. 5 and 6 respectively show the trainer and the trainee view of the MQIS substation at the start of the scenario (before the loss of the two transformers). The two views differ in that the trainer can view the "real" state of the grid (as simulated by Dynaωo), while the trainee only has access to SCADA data. Most notably, some current values are not available in the trainee view (shown with stars instead of values in Fig. 6) as there is no direct telemeasurements for those values. Those missing values should normally be filled by the state estimator, but at the time of writing, it has not yet been integrated in this training platform. Also, measurements/controls received/sent by the trainee through the SCADA interface can be delayed/dropped/corrupted in the information flow model, while the trainer can directly act on the true state of the simulation.

A domain specific language (DSL) has been designed to help the trainer to easily define training scenarios. The DSL definition of the currently studied scenario is shown in Algorithm 2. The current scenario is pretty straightforward, but the DSL allows for more complex scenarios, including the definitions of conditional events (e.g., events that occur on low voltage, or after the occurrence of another event). The switches opened in the DSL scenario are the switches 1 and 2 shown in Fig. 5 and are connected to the lost transformers.

For this training scenario, three possible corrective actions are suggested to the trainee:

- **Topological action:** the trainee can open the busbar coupler in the substation MQIS (switch 3 in Fig. 5) through the SCADA interface.
- **Redispatch:** the trainee can ask for two nearby generators to curtail their production (from 940 to 750MW each). Note that this action is not possible through the SCADA interface. Instead, the trainee must call the central dispatcher (role played by the trainer) who will perform the action.
- **Load reduction:** the trainee can act on the total system load by acting on the tap changers of the distribution transformers (max 5% reduction).

The trainee is free to use any combination of these suggestions. Fig. 7 shows two possible sequences that could occur depending on the decisions of the trainee. In the first sequence, the trainee decides to open the MQIS busbar coupler at t=40s. As the figure shows, this is sufficient to relieve the overload. In the second sequence, the trainee instead decides to perform a

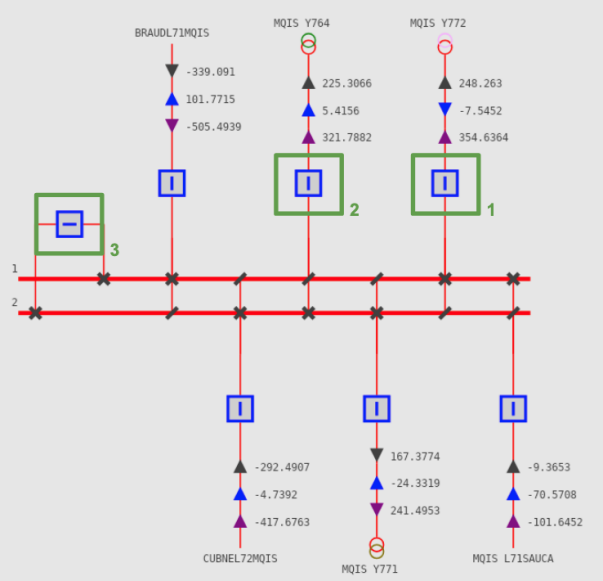

Fig. 5. Trainer view of the MQIS substation.

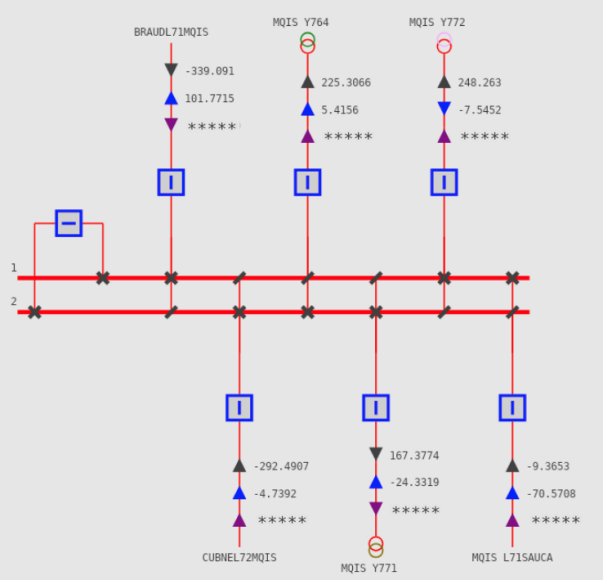

Fig. 6. Trainee view of the MQIS substation.

redispatch. He calls the trainer (who also plays the role of the central dispatcher) and ask for a reduction of the production of a nearby generator. At t=25s, the trainer starts to ramp down the production of this generator. As this is not sufficient, the trainee asks for a power reduction in a second generator, this starts to be implemented by the trainer at t=40s. As this is still not sufficient, the trainee launches a load reduction at t=53s, and at t=57s, the overload is finally resolved.

IV. Conclusion and Future Works

This paper presented a real-time cyber-physical simulation platform designed to serve as a digital twin of the French transmission grid. The main objective of the platform is to train operators and to test new automata and decision-support

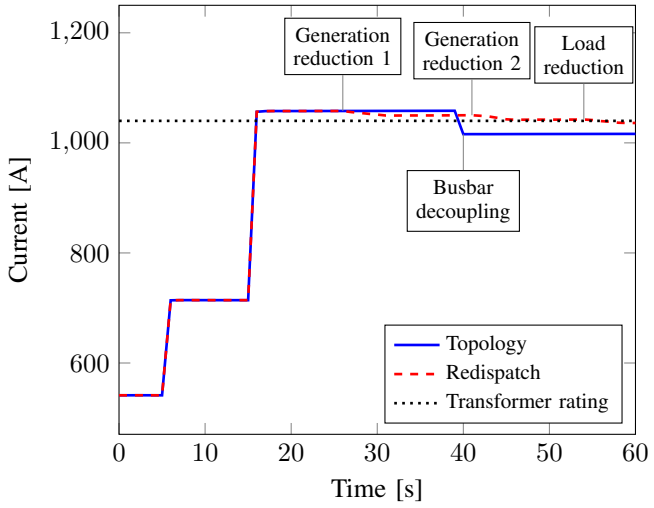

Fig. 7. Evolution of the current in the MQIS Y761 transformer in one scenario where the trainee opens the MQIS busbar coupler (full blue line), and in a scenario where the trainee performs generator and load reduction (dashed red line).

tools. This includes helping the operators to get used to and to trust the new tools.

The scalability of the platform (able to simulate a system with more than 6000 substations and 500k signal emissions per second[2]) has mainly been achieved through the use of information flow modeling instead of detailed cyber simulations (through a dedicated network simulator such as ns-3 or OMNeT++). This means that instead of modeling each cyber process at the protocol level, we model information flows using mathematical functions to represent delays, drops and data corruptions. These mathematical functions can be simply constant delays, but we have also extended it to include more complex stochastic processes.

The scalability of the platform has been demonstrated on a simple training scenario simulated on the full French network. From this, the obvious next step is to use the platform for the simulation of more complex scenarios including actions from more complex automata. To help with this, the capabilities of the platform will be extended in order to be able to replay real historical scenarios based on SCADA data from past events.

Another possible extension would be to implement a so-called "zoom capability", i.e. the ability to simulate part of the cyber network (e.g., a substation or group of substations) using a detailed simulator and the remaining of the network using the information flow model. This would allow for more precise modelling in a study area while still keeping the ability to simulate large networks. Finally, on a longer timescale, the platform could be further scaled up to simulate the whole European grid.

[2]These 500k signals actually include both 500k "physical" signals being sent directly to the game master and 500k equivalent "cyber" signals going through the information flow model and then being sent to SCADA interface.

REFERENCES

[1] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, 2021.

[2] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[3] A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 440–450, 2020.

[4] F. Sabot, P.-E. Labeau, J.-M. Dricot, and P. Henneaux, "Towards an efficient simulation approach for transmission systems with ICT infrastructures," *arXiv preprint arXiv:2311.14467*, 2023.

[5] Z. Liu, Q. Wang, and Y. Tang, "Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems," *IEEE Access*, vol. 8, pp. 95 997–96 005, 2020.

[6] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, 2015.

[7] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, and S. Shi, "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4893–4905, 2018.

[8] A. Guironnet, M. Saugier, S. Petitrenaud, F. Xavier, and P. Panciatici, "Towards an open-source solution using Modelica for time-domain simulation of power systems," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2018.