Flexible hardware-in-the-loop testbed for cyber physical power system simulation

Heqin Tong¹, Ming Ni², Lili Zhao¹, Manli Li¹
¹NARI Technology Co., Ltd, NARI Group Corporation, 19 Chengxin Road, Nanjing, People's Republic of China
²E-mail: ni-ming@agepri.sgcc.com.cn

Abstract: Nowadays, the power system is evolving into a complex cyber physical system with the closely merged physical system, information system, and communication network. It is critical to understand the connections between the power and cyber systems, and the potential impact of cyber vulnerability. In this study, a flexible hardware-in-the-loop (HIL) testbed is proposed for studying the cyber physical power system. By using the flexible interface, various co-simulation systems for different purposes are generated. Based on this testbed, three sample co-simulators are built as proofs. First, a HIL power and communication co-simulator with non-real-time synchronisation mechanism is introduced, and a case of false data injection attack on automation voltage control is studied. Then, a real-time power and communication HIL co-simulator is introduced, and a case considering the impact of communication bit error on the stability control system is simulated to demonstrate the performance of stability control equipment. Finally, another co-simulator for simulating the actual cyber-attack on the stability control system is introduced, and a case of a man-in-the-middle attack on the data link is simulated to demonstrate the impact of cyber-attack on the stability control system.

1 Introduction

With the deep mergence of physical system, information, and communication technology (ICT), the power system is evolving to the cyber physical power system (CPPS), which results in the fact that the control strategy and measurement data of the power system rely more on the information system and communication network [1, 2]. Owing to the close association between physical and cyber systems, the power system becomes increasingly vulnerable to cyber events and cyber-attacks. However, for the power system, the impact of the cyber events and attacks is not always clear enough to be studied analytically, so it is necessary to develop the testbed for the CPPS simulation. There are three ways to simulate the CPPS. One is simulating the CPPS with either power system or communication simulator. To do this, either the power system or cyber system model needs to be simplified, which will result in an inaccurate result. The second way is simulating the CPPS with both power and communication simulators, but separately. In this way, the simulation will be performed iteratively, and the information exchange between the simulators will be done manually, which is not efficient and hard to simulate the cascading failures within two systems. Therefore, the widely used way is the third one, i.e. the co-simulation.

Some developed co-simulation testbeds focused on the digital simulation which lack hardware interface to integrate the real-life equipment and cannot be used to evaluate and analyse the impact of the real-life components’ performance on the system, such as the real-life control equipment and communication equipment, private communication protocol, some cyber-attack behaviours etc. For example, in [3], the framework of a virtual control system environment provides a testbed for a large-scale control system test by using OPNET as the cyber simulator and PowerWorld as the power simulator; in [4], a framework of integrated cosimulation of power and ICT systems for real-time evaluation, which integrates a flexible communication environment, is utilised to evaluate the impact of ICT on the power system. Moreover, there are some other disadvantages, such as the shortage to create the model for complex interaction in a cyber-physical system (CPS) environment. For example, in [5], as the pre-set time point is adopted for synchronisation, the simulation errors may be accumulated in the framework of electric power and communication synchronising simulation; in [6], the global event list is adopted in the framework of global event-driven co-simulation for synchronisation during co-simulation, but ‘it does not help to remove errors introduced by simulators themselves’ [7].

Furthermore, some others apply real-life equipment instead of the simulation models to build hardware-in-the-loop (HIL) testbed. Compared with the testbed of digital simulation, HIL testbed provides more accurate performances for the equipment and simulated system and is closer to the practicality [8]. Especially, for the communication network simulation, the HIL testbed provides even more benefits in communication modelling, modelling capability, modelling granularity, and modelling reliability. For example, in [9], a HIL testbed of DiGSILENT and smart city testbed is used to examine the impact of cyber-attack on the GOOSE network in the substation; in [10], a HIL testbed of real-time digital simulator (RTDS) and OPNET is built to simulate the impact of cyber-attack on the Modbus/transaction control protocol; in [11], a HIL testbed for wide area measurement system is built to create dataset and analyse cyber-attack; in [12], a survey on testbed for smart grid CPS reviews and evaluates some platforms of the testbeds; in [13], a non-real-time HIL testbed is proposed, in which software and simulation tools replace the expensive real-time component, and synchronisation component is provided to ensure the accurate behaviour during the simulation; in [14, 15], the testbed is built for cyber security evaluation; in [16], a real-time HIL co-simulation testbed using RTDS, phasor measurement unit (PMU), phasor data concentrator (PDU), satellite-synchronised clock, DeterLab, and RT-VSMAC has been built to analyse the cyber-attack, and the impacts of cyber-attack of denial-of-service and man-in-the-middle (MITM) on power grid are simulated. In general, the communication simulator, in the HIL CPPS testbed, consists of the real network and the virtual network, and by mapping the real nodes into a virtual network, the real network and the virtual network can be combined together [17]. Since the real network is running in real-time, the virtual network should coordinate with that in the real-time environment and the same with the interface between the virtual network and real network [17].

The most tested frameworks mentioned above have the following disadvantages: (i) lack of flexibility to integrate different simulators; (ii) lack of the interface to support various hardware
and communication protocols in the cyber system; (iii) some of them lack the ability to introduce real network attack into the simulation. Therefore, we develop a flexible HIL testbed for CPPS simulation. In this testbed, the flexible interface offers users the capabilities to build a simulation system for their own purpose. To illustrate the flexibility of this testbed to integrate different simulators, a scenario of automation voltage control (AVC) simulation is created as the proof of non-real-time HIL co-simulation; a scenario of stability control system over synchronous digital hierarchy (SDH) network simulation is created as the proof of real-time HIL co-simulation; and a scenario of MITM attack on power system stability control simulation is created as the proof of cyber-attack co-simulation, which can demonstrate the attacker’s attacking process.

2 Components of the HIL testbed

In the testbed, the communication simulator operates in a real-time environment, and the other parts are connected to it through the flexible interface which offers a different interface for various protocols, communication modes, products etc. Thus, a flexible platform is built for cyber-attack analysis, power system assessment, equipment testing etc. The testbed contains five layers: (i) the power simulation layer; (ii) the power control layer; (iii) the communication simulation layer; (iv) user control panel layer; and (v) interface layer. The interconnections and information transmissions among the different layers are shown in Fig. 1.

2.1 Power simulation layer

The power system is modelled in the power simulation layer. The power simulator can run in non-real-time or real-time.

When it runs in non-real-time, the power devices should be modelled in the power simulator, and the synchronisation mechanism should be considered to complete the co-simulation task with other simulators. In the sample testbed, DigSILENT Power Factory is used as a non-real-time simulator for non-real-time co-simulation. In the DigSILENT Power Factory, the power grid elements and power devices such as transmission line, bus, generator, transformer etc., are modelled in the same simulator, and the interaction with other simulator is via software interface or communication packets [17].

For real-time simulation, a typical real-time simulator, such as RTDS operates at a time step as low as 50 ns. Furthermore, when the RTDS is used to simulate the power grid, it provides the digital and analogue signal input/output ports for high-speed data exchange with real-life equipment [17, 18].

2.2 Power control layer

For different simulation purposes, the power control layer of the platform offers a flexible configuration mode, which integrates some power control applications, such as automatic voltage control (AVC), power stability control, distributed load control etc. The control logic is modelled as a control centre or distributed controller and embedded into the control layer. By changing the control logic, the different control decisions can be made for different application. In this study, the power stability control and distributed load control are presented as examples to demonstrate the flexible configuration for different applications:

(a) Power stability control: The power stability control nodes obtain the power grid status from the power simulator. By analysing the status, the control nodes match the control strategies, which are beforehand stored, and send out control command. It is a centralised control mechanism.

(b) Distributed load control: It is a large-scale source-grid-load friendly co-operative system for stability control. The control centre acts as a manager. On the other hand, the control nodes get the information from the control centre and execute load control.

2.3 Communication simulation layer

In this testbed, communication simulator and communication equipment are used for the communication network simulation, which provides a virtual link among the devices of the power control system. As the communication simulator usually runs in real time and provides the interface for real-life equipment, the real-life packets can pass through the virtual communication network, which is designed in the simulator, and some real-life communication hardware. In this study, the virtual SDH network and virtual data dispatching network functions are developed in QualNet. As a well-known simulator, QualNet provides plenty of wired and wireless network models and protocol models for wired, wireless, and hybrid network analysis [17, 19], and can be used to simulate transmission delay, transmission interruption, and bit errors.

Since it provides stable and point-to-point secure channels, the SDH technology is widely used for power stability control. The E1 channels, which are assigned for each stability control business, provide a 2 Mbps data rate for digital transmission. A bunch of E1 channels is multiplexed into the SDH channel and transmit in the SDH network. To simulate the SDH network, we create an SDH network model with a self-healing ring protection function, which is designed by using the static route model provided by the simulator [17, 20].

2.4 User control panel layer

The user control panel provides the interface for power and communication systems’ configuration; the simulation mode of non-real-time and real-time selection; the control application setting; co-simulation procedure and data transmission management etc.

2.5 Interface layer

The interface layer is the key layer for the flexible HIL co-simulation platform, which connects the above four layers together, and provides various entry points for different applications and products. By this entry, the real control command or measurement data, which is generated in the real-life devices, can be simulated in the virtual network. As the real equipment is in a real-time environment, the virtual network should coordinate with that in the real-time environment, and the same with the interface between the virtual network and real network [21]. Thus, high efficiency and real-time HIL simulation interface are required with the function of packet converting from the real communication packet to the virtual packet. The existing HIL interface may be classified into three types [21].

- High-level architecture (HLA) interface, which runs in the federal architecture through run time infrastructure. Although HLA became an IEEE standard [21, 22], it also has some shortages, such as not fit for some time critical simulation (millisecond time scale).

- System-in-the-loop (SITL) interface, which provides an interface between the physical hardware and virtual network. Via the interface, Ethernet packets can be transmitted into the virtual network, and it combines real-life network and virtual
network as a whole [21–23]. However, the SITL interface can only connect to Ethernet.

• Self-defined interface, which is developed to allow external hardware to access the virtual network [21, 22]. Compared with the two interfaces above, the self-defined interface is much more flexible but needs a lot of additional coding work [21].

Based on the interface, power simulator and communication simulator can be combined together and became a testbed for co-simulation.

In this study, the self-defined HIL interface is designed, which contains a hardware interface/protocol converter and a data interface for a communication simulator. The data interface is used to receive/send an Ethernet packet for the communication simulator. In the communication simulator, a virtual network is built, and one of the virtual nodes is mapped to the real network node with a real device connected. By this virtual node, the Ethernet packet is converted into the virtual packet, and transmitted in the virtual network; or the virtual packet is converted into the Ethernet packet, and transmitted back to real network node [17].

However, there are many other communication protocols and architectures in the power system rather than the Ethernet protocol, such as Modbus, DNP3, IEEE C37, IEC 61850, GOOSE, sampled measured value (SMV) etc. Thus, the protocol converter is required, which works as another interface of real-life hardware interface for hardware connection and protocol conversion. In the sample co-simulators, the protocol converter for stability control equipment is developed. Depending on the communication direction, the protocol converter transforms either the real control command or measurement data into user datagram protocol (UDP) packets or the UDP packets into the real control command or measurement data, which is discussed in detail in Section 4. Moreover, the protocol converter can also be responsible for the synchronisation of the data exchange between the simulator and the real-life hardware [21], which is discussed in detail in Section 3.

3 Scenario 1: non-real-time HIL Co-simulation

In some cases, the power simulator cannot run in real-time because of the limitation of the simulator’s speed, while the communication system with communication equipment runs in real-time so that a non-real-time HIL co-simulator should be built with an appropriate synchronisation mechanism. To illustrate how to build the non-real-time HIL simulator based on the testbed, a case of false data injection attack (FDIA) on AVC is studied. AVC signals are transmitted through an Ethernet-based network.

3.1 Structure of non-real-time HIL co-simulator

As shown in Fig. 2, the non-real-time HIL co-simulator consists of power simulator, power control centre, user control panel/interface, communication simulator, attacker, and routers, which work as both the communication equipment and the self-defined HIL interface. In the co-simulator, DiGSIILENT is applied as a power simulator to simulate power grid; power control centre simulates the function of AVC; QualNet is applied to build and simulate a virtual communication network; cyber-attacker is a programme running on another computer which can change the contents of communication packets; user control panel is loaded on one computer, which configures the power system, power control centre, and communication system, and manages synchronisation and the simulation procedure. The communication network is built by the real routers and the virtual network, which runs in real-time. Since the measurement data and AVC control command are transmitted over the dispatching data network, a virtual Ethernet is developed for communication simulation. The real routers are applied as a part of the communication system. To emulate the real communication system, Router1 and Router3 work as customer edge router (CE router), which connect the control device and power simulator in the power domain; and Router2 works as a provider edge router (PE router), which provides an entrance for the on-site power information transmitted to power control centre via the core communication network. As the PE router provides interfaces for many customers, it may give the attacker the opportunity to eavesdrop or attack the information transmitted in the network. So, the attacked computer works as a part of a communication system to emulate the cyber-attack in the co-simulation system.

During the co-simulation, the DiGSIILENT sends the power status data to the AVC control centre through the user control panel with time-stamp added; then router in the communication system forwards the data packets to the virtual Ethernet through the data interface provided by QualNet; to emulate the attacker, the router is configured to filter the packets and forward some special packets to the attacker computer where packets are analysed and changed; after the packets passing through the virtual network, the data packets are transmitted to the AVC control centre; then, the AVC control centre analyses the power status data, and sends the control packets to the communication simulator with another time-stamp; passing through the virtual Ethernet and router, the control packets are forwarded to the user control panel; using the time-stamp information, the simulation time can be synchronised, and the transmission time delay can be calculated; according to the simulation time and time delay, the DiGSIILENT performs the next round of power simulation. Thus, a non-real-time HIL testbed for close loop co-simulation is built.

Building an accurate, efficient and inexpensive HIL co-simulation testbed could be sometimes contradictory. However, by using the non-real-time HIL testbed, researchers can apply an inexpensive simulator to simulate some complex CPPS scenarios, and some CPPS scenarios with compound power and cyber system events will be beneficial for this testbed, in which the ICT events are not time-critical and ICT condition of the HIL testbed is manageable during the power simulation.

3.2 Synchronisation mechanism of non-real-time HIL co-simulator

As the power simulator runs in non-real-time, while the communication simulator runs in real-time, it is hard to synchronise them by the known synchronisation mechanism. Therefore, a new synchronisation mechanism is proposed in which a virtual communication simulation is created. This time line keeps the synchronisation with the power system simulation time line and matches the real-time communication simulation.

Fig. 3 shows an overview of the synchronisation mechanism for the non-real-time HIL simulation. A global event queue is set for power and communication simulation before the simulation begins. Moreover, there are three time lines for power simulation, real-time communication simulation, and equipment simulation, separately. During co-simulation, Event 1 is the pre-known power event and set in the global event queue first. Then, the simulation will follow the step sequence marked in the figure. When the power simulation runs first to the time-stamp of Event 1, the global event queue will suspend the power simulator and transmits a real power control command to the communication system. At the same time, power
status at time-stamp of Event1 is stored for next round power simulation. The control command transmitted to the communication system will be encapsulated with the time-stamp of TG for the physical time of the power simulator and time-stamp of TE for power simulation time. The communication simulator receives the packet and added the new time-stamp of TR for the physical time of receiving the packet; then it reads the time-stamp of TE and the new time-stamp of TC for communication simulation time. After the communication simulation, the packet will send back to power simulator, which will decode the packet and buffer the control command. When the power simulator receives the packet, a time-stamp of TA is created.

So, time latency $T$ of packet transmission in the HIL simulation network can be calculated as

$$T = (TR - TG) + (TA - TC) \quad (1)$$

Then the Event 2 is set in the global event queue at the time point of $TE + T$. After that the power simulator continues the power simulation from Event 1 to Event 2 and processes the control command, which is transmitted from the communication system.

Since the simulation time of non-real-time simulation system runs a long lag of the physical time, in this synchronisation mechanism, time-stamps are inserted into packets for matching the physical time to simulation time, and the co-simulation with both non-real-time simulator and real-time simulator can be achieved.

3.3 Simulation case

In this case, the IEEE 39-bus model is used, as shown in Fig. 4 [17]. The AVC control located in the power control centre calculates the voltage adjustment values for buses every 5 s and sends the values to corresponding generators.

The non-real-time HIL co-simulation framework is shown in Fig. 5. The AVC control signals and measurement data are transmitted through the virtual dispatching data network, which is built in communication simulator and real-life routers. In usual, the regular path for measurement data transmission is from CE router (Router1), via the PE router (Router2) and the virtual core network of the provider, to the CE router (Router3) of the power control centre. After receiving the measurement data, the AVC control center will transmit control command back to the power simulator via the same route. However, if the attacker invades the PE router, filters the packets by their source internet protocol address and port number, and creates the by-pass traffic focusing on the specific power node measurement data for an FDIA attack, the AVC control centre would make a wrong control decision due to the fake measurement data. By using this method, the attacker may attack the power system more secretly than making fake control command packet.

3.4 Result of simulation

(i) No FDIA attack on the router: If no attacker hacks into the communication system, the measurement data is transmitted to the AVC control centre properly, and every 5 s the calculated control values will be sent to the corresponding generators correctly. The voltage magnitude in bus 31 is shown as the curve without sawtooth in Fig. 6.

(ii) FDIA attack on the router: If the attacker attacks Router2 and creates by-pass traffic focusing on the measurement data of generator G1, the attacker may eavesdrops the measurement data and fudge the measurement data 5 s after simulation beginning. By the simulation, the voltage magnitude in bus 31 is shown as the curve with sawtooth in Fig. 6.

By analysing the result, we can see that the attacker can change the configuration of routers to attack the communication system. In this case, the attacker focuses on some special packets and successfully manipulates the measurement data to mislead the control centre to make an inaccurate decision. To avoid the attack, encrypting the transmitted packets is required. Furthermore, by this framework, real-time and non-real-time simulators can co-operate co-ordinately, which offers great flexibility to simulate compound CPPS system.
4 Scenario 2: real-time HIL co-simulation for a stability control system

In this scenario, the stability control system contains two layers, the main station and execution station. The execution station sends the measurement data to the main station; the main station judges the control strategy based on the measurement data and sends a control command to the execution station; the execution station executes the control command of generator tripping or load shedding from the main station.

4.1 Implementation of real-time HIL co-simulator

The stability control packages are transmitted through the E1 channel via the SDH network, which is encapsulated in private communication protocol. To include the actual stability control stations in the simulation, a special protocol converter is developed for converting private protocol data through the E1 channel to SOCKET UDP packets through Ethernet.

Fig. 7 shows the framework of a real-time HIL co-simulator, which consists of SDH equipment, SDH protocol converter for self-defined HIL interface, RTDS, QualNet, stability control stations, and their associated equipment. The real-time synchronisation mechanism is applied, and the E1 channels are used for the interactions in the SDH network.

In the framework, the power grid and related power control components are modelled in the RTDS. The analogue output from the RTDS is amplified by the power amplifier and sent to the stability control stations as input. The stability control stations are connected to RTDS through the switch signal converter for the control command input/output. Also, E1 cables connect SDH equipment and stability control stations for communication purpose. The actual frequency of stability control stations sending/receiving data to/from the E1 channel is 0.833 ms. The throughput via the E1 channel is about 2 Mbps.

As both power simulator and communication simulator run in real-time, the co-simulation system runs with real-time synchronisation mechanism. The signal transmission process is as follows: the digital measurement data from RTDS is sent to the execution stations through power amplifier; then the measurement data enters SDH equipment through the E1 channel, and is converted to SOCKET UDP packets through the protocol converter; the SOCKET UDP packets are sent to the main station side through the virtual communication network simulated in QualNet; then the SOCKET UDP packets are converted to E1 data through the protocol converter, and the data is sent to the main station via SDH equipment; the main station generates the control command data based on the measurements, and sends the command back to execution stations through the reverse transmission process described above; finally RTDS receives the control signal through a switch signal converter, and continues the power simulation.

4.2 Simulation case 1: impact of communication bit error

4.2.1 Case introduction: In this case, how the communication bit error in the control command transmission affects the stability control is simulated. A power grid in a province of China is used as an example, and a structure of the stability control system is shown in Fig. 8.

As shown in Fig. 9, the stability control stations communicate with each other over E1 channels. The E1 channels are multiplexed into the SDH frame and transmitted through the SDH nodes. At the terminal node of the SDH, the E1 channels are de-multiplexed from the SDH frame. The SDH network contains two layers: the core layer (the SDH backbone ring), and the access layer (the SDH branch). In this case, the distance of the communication line from the main station C to the execution station E is 200 km and passing through five SDH nodes. The total communication delay from the main station C to the execution station E can be calculated by the engineering calculation as shown in (2)

\[
T = \frac{n}{c} \times L + N \times t
\]

where \( T \) is the total time delay; \( n \) is the index of refraction of the optical fibre, whose typical value is 1.48; \( c \) is the light speed in vacuum, which is \( 3 \times 10^8 \) km/s; \( L \) is the distance of the optical fibre; \( N \) is the number of the SDH node in the path of transmission; \( t \) is the data transmission delay of the SDH equipment, whose
Table 1 Simulated communication delay and the total execution time in three states

| Case No. | Communication delay, ms | Total execution time, ms |
|----------|-------------------------|--------------------------|
| case a   | 1.51                    | 1133.4                   |
| case b   | 1.52                    | 1140.3                   |
| case c   | 1.51                    | 1232.0                   |
| calculated | 1.49                  | —                        |

Fig. 10 Simulation results of the impact of BER on power system stability control

average value is 0.1 ms. Through engineering calculation, the total communication delay is 1.49 ms.

In the simulation, power failure of a three-phase short-circuit fault happens on 500 kV line A–C at 0 s. The protection relay trips off this line at 100 ms. To deal with this failure, the control strategy is set for load shedding in the execution stations D and E. The main station C obtains the status of power failure, searches for the correct control strategy, and sends out the control commands of load shedding to the execution stations D and E.

The transmission of the control commands from the main station C to the execution station E will pass through link S as shown in Fig. 9. The bit error ratio (BER) in the SDH backbone ring is assumed at $1 \times 10^{-11}$, and three communication states in link S are simulated [21].

(a) Link S in a normal state, the BER is $7 \times 10^{-4}$.
(b) In link S, if there is a communication event happening at 0 s, where the link attenuation increased, the BER increases to $7 \times 10^{-4}$.
(c) In link S, if there is a serious communication event happening at 0 s, the BER increases to $1.56 \times 10^{-3}$ [24].

4.2.2 Results of simulation: The simulated communication delay and total execution time in these three states are shown in Table 1. The simulated communication delay closes to the engineering calculation result.

In the normal operation, after the three-phase short-circuit fault happens, the main station C sends out the control command of load-shedding to the execution station E via the communication network. As the communication status is normal, the execution station E can execute the load-shedding properly. The result of power simulation is shown as the blue curve without sawtooth in Fig. 10.

When the BER reached $7 \times 10^{-4}$ in link S, by the HIL co-simulation, it shows that the effect of load-shedding is almost the same as in normal status. The result of power simulation is shown as the brown curve without sawtooth in Fig. 10.

However, if the BER reached $1.56 \times 10^{-3}$ in link S, the HIL co-simulation shows that execution station E discards large amounts of data that contains error bit, which increases the processing time of the station and results in much longer total execution time. The result of power simulation is shown as the curve with sawtooth in Fig. 10.

By analysing the result, we can find that the SDH network provides a stable communication delay, but the error packets would impact the equipment execution time seriously, which may affect control when the BER increases. It is hard to create a digital model to describe the equipment execution time for simulation. However, in this HIL testbed, the real equipment can be included in the simulation framework, its execution time can be easily captured and its impact can be accurately simulated.

5 Scenario 3: cyber-attack HIL co-simulation for a stability control system

As proof of flexible HIL testbed for cyber-attack analysis, a scenario of the MITM attack to the stability control system is studied by using the same example in Section IV.

5.1 MITM attack

A MITM attack is an attack, in which the attacker secretly makes the independent connection between two endpoints. The MITM attacker compromises the communication and relays information between two victims, which gives the attacker an opportunity to send fake packages [25]. In the real world, for stability control, the equipment connects with each other through the E1 channel via the SDH network. The attacker could use some hardware access to invade the E1 channel. A successful attacker could hijack the transmitting packets or create fake messages, including important measurement and control command.

In the existing platform, cyber-attack is simulated by the created attack model in the simulator, and the procedure of how the attacker attacks the ICT system is ignored. Especially, there is little example demonstrating how the attacker invades the SDH system via its E1 channel. In this scenario, the HIL testbed is used to emulate the detailed procedure of attack, as well as the attack of invading into the real life E1 channel to attack the power system.

5.2 Implementation of HIL co-simulation for cyber attack

The framework for MITM attack co-simulation is built as shown in Fig. 11, which consists of SDH equipment, SDH protocol converter for self-defined HIL interface, RTDS, stability control equipment, QualNet, and MITM attack computer. The MITM attack computer is located between the QualNet and SDH protocol converter to emulate the MITM attack on the link S as shown in Fig. 12. It adopts a real-time synchronisation mechanism, and the communication in the SDH network is via the E1 channels.

The signal transmission process, in this case, is similar to that in Section 4, except that encapsulated SOCKET UDP packets, which should be transmitted from the communication simulator to the protocol converter, are transmitted to the attack computer where the attacker eavesdrops and tampers the information in the SOCKET UDP packets, and sends the fake packets to the protocol converter.

5.3 MITM attack for Mal-operation

When the power system runs in normal conditions, the stability control stations will not act. Main station C sends the time setting through its E1 channel. In this scenario, the attacker compromises the communication and relays information between two victims, which gives the attacker an opportunity to send fake packets [25]. In the real world, for stability control, the equipment connects with each other through the E1 channel via the SDH network. The attacker could use some hardware access to invade the E1 channel. A successful attacker could hijack the transmitting packets or create fake messages, including important measurement and control command.

In the existing platform, cyber-attack is simulated by the created attack model in the simulator, and the procedure of how the attacker attacks the ICT system is ignored. Especially, there is little example demonstrating how the attacker invades the SDH system via its E1 channel. In this scenario, the HIL testbed is used to emulate the detailed procedure of attack, as well as the attack of invading into the real life E1 channel to attack the power system.
packets to the execution stations A, B, D, and E under normal conditions. However, during the MITM attack, the attacker manipulates the load shedding command instead of time setting packets to the stability controller in the execution station E. Then, station E executes the load shedding by fault as shown in Fig. 13a, which causes power system state change as shown in Fig. 13b.

5.4 MITM attack for refuse-operation

In Section 4, the power failure of three-phase short-circuit fault is simulated. To deal with this failure, the control strategy is load shedding in the execution stations D and E.

Under normal operating conditions, main station C sends load shedding command packets to execution stations D and E. Load shedding commands are executed normally and the simulation result of the power system is shown as the curve without sawtooth in Fig. 14a. However, during the MITM attack on the E1 channel from the main station C to the execution station E, the attacker manipulates the time setting packets instead of the load shedding command. Then, the load shedding command to station E is not received and executed (as shown in Fig. 14a), and the simulation result of the power system is the curve with sawtooth shown in Fig. 14b.

As shown in Figs. 13 and 14, cyber-attack on the communication system could mislead the equipment to execute wrong control actions and affect power system. By using the testbed, the real attack can be tested and analysed, which help to evaluate cyber security and find out the weakness of the system. Moreover, the equipment and communication protocol can be tested, and the security strategies can be evaluated on this testbed.

6 Conclusions

In this study, a flexible HIL testbed for CPPS is introduced, which can be applied for analysing the effect of a cyber-event, such as cyber-attack and communication failures, on the power system. As the testbed provides a flexible interface, it can be used to build various frameworks for various simulation missions. By using this testbed, three sample HIL co-simulators are built and tested, i.e. non-real-time HIL co-simulator for AVC control, real-time HIL co-simulator for the stability control system, and cyber-attack HIL co-simulator for the stability control system.

The future work is to extend the communication technologies supported by the testbed, such as software defined network, and expand the application field, such as comprehensive energy system simulation which includes other types of energies, such as gas, heat etc.

7 Acknowledgments

This work was supported by the Key Projects of National Natural Science Foundation of China (61833008) ‘Research on Cyber-Physical Security Theories and Active Defense Technologies for Smart Grids against Cyber-Attacks’; Project of State Grid Corporation of China ‘Identification Method of Malicious Attack on the Power Grid and Active Defense Method on the Power Grid Side’; and the Project of Jiangsu Economic and Information Technology Commission ‘Research of Key Technologies and Platform Development of Cyber Physical Power System Co-Simulation’.

Fig. 12 Topology of SDH network

Fig. 13 Result of MITM attack for Mal-operation
(a) Stability control stations operation by fault, (b) Power system state change under a MITM attack

Fig. 14 Result of MITM attack for refuse-operation
(a) Stability control stations operation by fault, (b) Result of the power system in a MITM attack
8 References

[1] Liu, C.-C., Stefanov, A., Hong, J., et al.: ‘Intruders in the grid’, IEEE Power Energy Mag., 2012, 10, (1), pp. 58–66
[2] Zhao, J.H., Wen, F., Xue, Y., et al.: ‘Modeling analysis and control research framework of cyber physical power systems’, Autom. Electr. Power Syst., 2011, 35, (16), pp. 1–8
[3] McDonald, M., Conrad, G., Service, T.C., et al.: ‘Cyber effects analysis using VCSE’, Tech. Rep. SAND2008-5954, 2008
[4] Georg, H., Muller, S.C., Rehtanz, C., et al.: ‘Analysing cyber-physical energy systems: the INSPIRE cosimulation of power and ICT systems using HELA’, IEEE Trans. Ind. Inf., 2014, 10, (4), pp. 2364–2373
[5] Hopkinson, K., Xiaoru, W., Giovanini, R., et al.: ‘EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components’, IEEE Trans. Power Syst., 2006, 21, (2), pp. 548–558
[6] Lin, H., Veda, S.S., Shukla, S.S., et al.: ‘GECO: global event-driven cosimulation framework for interconnected power system and communication network’, IEEE Trans. Smart Grid, 2012, 3, (3), pp. 1444–1456
[7] Lin, H., Sambamoorthy, S., Shukla, S., et al.: ‘Power system and communication network co-simulation for smart grid application’. Innovative Smart Grid Technologies, Medellin, Colombia, 2011, pp. 1–6
[8] Jablowski, B., Spiniczky, O., Kurech, M., et al.: ‘A hardware-in-the-loop co-simulation architecture for power system applications in virtual execution environments’. Modeling and Simulation of Cyber-Physical Energy Systems, Berlin, Germany, 2014, pp. 1–6
[9] Sun, C.C., Hahn, A., Liu, C.C.: ‘Cyber security of a power grid: state-of-the-art’, Internal J. Electrical Power Energy Syst., 2018, 99, (3), pp. 45–56
[10] Chen, B., Pattanaik, N., Goulart, A., et al.: ‘Modeling of intrusion and defense for assessment of cyber security at power substations’, IEEE Trans. Smart Grid, 2012, 10, (5), pp. 2444–2453
[11] Liu, R., Srivastava, A.: ‘Integrated simulation to analyse the impact of cyber-attacks on the power grid’. 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Porto, Portugal, 2018, pp. 1–5
[12] Liu, R., Vellaithurai, C., Biswas, S.S., et al.: ‘Analyzing the cyber-physical impact of cyber events on the power grid’, IEEE Trans. Smart Grid, 2017, 6, (5), pp. 2444–2453