Methodology for P&C cyber security studies using real-time digital simulation

Li, Jianing; Yang, Conghuan; Kong, Dechao; Mann, Stuart; Zhang, Xiao-ping

DOI:
10.1049/joe.2018.0273

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Li, J, Yang, C, Kong, D, Mann, S & Zhang, X 2018, 'Methodology for P&C cyber security studies using real-time digital simulation', *The Journal of Engineering*, vol. 2018, no. 15, pp. 1130-1134.
https://doi.org/10.1049/joe.2018.0273

The Journal of Engineering

The 14th International Conference on Developments in Power System Protection (DPSP 2018)

IET Journals
The Institution of Engineering and Technology

Methodology for P&C cyber security studies using real-time digital simulation

eISSN 2051-3305
Received on 4th May 2018
Accepted on 23rd May 2018
E-First on 7th September 2018
doi: 10.1049/joe.2018.0273
www.ietdl.org

Jianing Li[1], Conghuan Yang[1], Dechao Kong[2], Stuart Mann[2], Xiao-Ping Zhang[1] ✉

[1]*University of Birmingham, UK*
[2]*National Grid, UK*
✉ *E-mail: x.p.zhang@bham.ac.uk*

Abstract: With the smart grid development, advancements in deeply integrated information and communication technology (ICT) provide enhanced system awareness, effective decision-making support and high-performance protection and control (P&C) to improve operational reliably and stability of the modern power systems. To manage the risks relevant to the existing industrial P&C systems, it is of high necessity to develop a methodology of cyber security testing for industrial P&C systems. This methodology will be rolled out to continue to evaluate the risks for the next-generation industrial P&C systems when new ICTs are introduced e.g. IEC 61850. This study summarises the main purpose, scope of work of an innovation project in collaboration with National Grid. This on-going project is to develop such a methodology using the state-of-art real-time digital simulation to conduct hardware-in-the-loop testing.

1 Introduction

In recent years, research on cyber security for smart grids has shown that intentional attack could bring significant impact to power system reliability and stability. As a result, it could lead to further damage to the benefits of a utility and its stakeholders, e.g. damage to the reputation of a utility and economic loss to its customers. In [1], the authors investigated the impact of coordinated cyber-attacks on state estimation. Conditions to reproduce stealthy attacks targeting robust state estimators are determined whilst the phasor measurement unit assisted solutions to diagnose the attack are discussed. Attackers who have direct access to the back end system or field equipment may even modify the grid configuration for wider area physical impact on grid operations, which could result in a further economic loss to the market [2, 3]. Similarly, denial of service attacks could be raised in the absence of any component in the communication network, which leads to significant delays or impairs legitimate services [4, 5]. From protection and control (P&C) point of view, it is also important to verify the integrity of device configuration, algorithms and application before deployment and preferably throughout the operation [6]. For example, tampered relays can lead to mal-operation of the corresponding circuit breakers, which can cause cascading wider area system failures.

The risks introduced by vulnerabilities in information and communication technology and P&C should be carefully managed. To provide effective management, it is critical to understand the complexity of cyber physical systems with respect to a number of key areas that include:

- the physical and logical architecture of the system
- the actual services and vulnerabilities presented by each device
- the potential impacts of a series of cyber events engineered to exploit the vulnerabilities that have been proved to exist

Without a proper understanding of the system and methodology for management of those risks, there is significant potential to lead to a series of power system incidents and even severe system blackouts, which inevitably bring certain or even significant losses to a transmission owner and its stakeholders. In this case, in order to help understand the complex relation between cyber and physical equipment, a fit for purpose cyber physical testbed should be developed for simulating the power system together with physical hardware connected and operated in real time. This study summarises the on-going work of developing such a methodology using the state-of-the-art real-time digital simulation (RTDS) to conduct hardware-in-the-loop (HIL) testing with the following technical considerations:

- Design and implementation of the RTDS-based HIL testbed which is fit for the purpose.
- Determination of vulnerabilities that exist within a system.
- Design of test scenarios to conduct cyber events and evaluation of their impacts on the reliability, security and safety of network operation for conventional P&C systems as well as IEC-61850 based P&C systems.

2 Implementation of the RTDS-based HIL testbed

RTDS has been used for performing HIL experiments in a wide range of applications [7, 8]. Through different interfaces, the RTDS can be used to interact with different types of physical equipment in different ways. Two main types of RTDS-based HIL testbeds are introduced. To help understand the system, a model of standard Kundur's two-area four-machine system is implemented in RTDS that includes the high-voltage components, e.g. synchronous generators, transmission lines, circuit breakers, instrumental transformers, power transformers, static load, and plus differential P&C functions.

2.1 RTDS-based HIL testbed through the electrical interface

Electrical interfaces include both analogue and digital I/O cards. They allow RTDS to establish bi-directional communication through both analogue and digital signals. A schematic diagram of the HIL testing platform is shown in Fig. 1.

The two-area power system and associated current transformers (CTs) are all modelled in RTDS. The CTs are providing secondary current measurement signals to external devices through the analogue electrical I/O interface. As the analogue output signal from the analogue I/O interface is ±10 V whilst for protection relays, nominal voltage and current level for the secondary side are usually 110 V and 1 A, respectively. Therefore, an amplifier is used as an interface between RTDS and protection relays. The trip and reclose signals provided by a relay can be sent back to the RTDS through the digital I/O interface. It can be used to send or receive binary signals to or from relays. The received signal is then applied

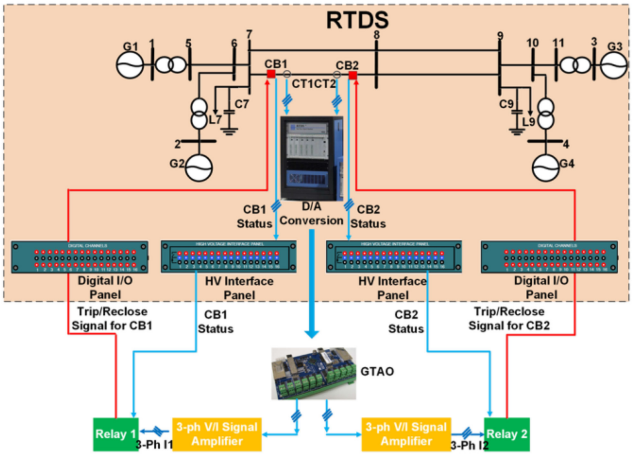

Fig. 1 *Schematic for RTDS based HIL testbed through an electrical interface*

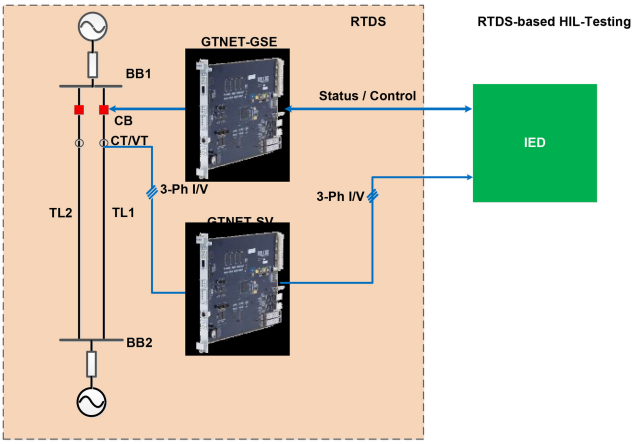

Fig. 2 *Schematic for RTDS based HIL testbed through the IEC-61850 interface*

directly to control the operation of the circuit breaker. The circuit breaker status from the RTDS can also be sent back to the relay.

By setting up the testing platform, relays are behaving in such a way as if they were installed and deployed in an actual substation.

The triggering of various faults, tampering and disabling events in power systems is configured and fully customisable within the RTDS. All electrical variables within the power system, analogue input/output signals, and digital input/output signals can be readily measured in real time. This is useful in terms of the identification of potential impact to the system from tampered or disables equipment/signals.

2.2 RTDS-based testbed through IEC-61850 interface

As shown in Fig. 2, the RTDS will be acting as an IEC-61850 compatible IED and communicate with another IEC-61850 compatible IED through IEC-61850 interface card. The RTDS IEC-61850 interface card is compatible with IEC-61850 communication with sample values (SVs), generic object oriented substation events (GOOSE) and manufacturing message specification. A GTNET-SV card will be able to transfer sampled values for voltage and current signals to the connected IED whereas a GTNET-GSE card can send and receive status or control signals to or from the IED. By using the IEC-61850 protocol, only Ethernet communication is required and hence, from cabling point of view, a lot of effort can be saved compared with a traditional electrical cabling setup.

Apart from the communication between the RTDS and IEDs, a network environment needs to be established as required by IEC-61850. In this case, as shown in Fig. 3, the testing network environment has been setup. All the devices are connected to a network switch under a router. A global positioning system clock is used for time synchronisation as the grandmaster with an IP

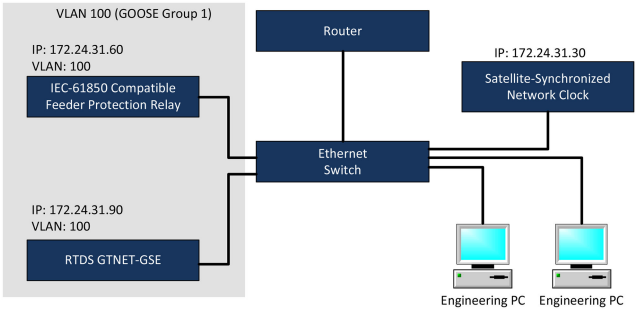

Fig. 3 *Network topology for RTDS-based HIL testbed*

address of 172.24.31.30. Engineering personal computers are also connected to the network switch. As an example, the IED to be tested is an IEC-61850 compatible feeder protection relay. It is compatible with the IEC-61850 GOOSE messaging protocol. Together with the RTDS GTNET-GSE card, both devices are under virtual local area network 100, which is a subgroup for GOOSE messaging devices to reduce performance impact from the multicast packet storm.

2.3 RTDS supervisory control and data acquisition (SCADA) system

A SCADA system, as shown in Fig. 4, is developed in the RTDS software RSCAD to enable monitoring and the issuing of process commands, such as controller set point changes, different settings of fault conditions, and tampered scenarios. The SCADA system developed in RSCAD grants users a graphical user interface for a high-level process supervisory management in real time. The following information can be obtained from the SCADA implementation in RSCAD:

- Active and reactive power output from synchronous generators.
- Magnitude and angle of bus voltages.
- Status of the circuit breaker.
- Active and reactive power through transmission lines.
- Normal/overloading condition of transmission lines.

In addition, the supervisory control, data acquisition, and condition monitoring for various testing scenarios can also be achieved and customised for specific testing condition settings.

2.4 Design test cases

When designing test cases, it is very important to identify where the risks would come from. For general equipment, it would usually be three types, input, output and internal software or algorithm.

To analyse an IED device, e.g. protection relay, by looking into Fig. 5, the potential risk could come from the following different areas: (i) *Analogue inputs*: These signals usually carry current or voltage data. The magnitude or phase could be altered or completely changed. (ii) *Protection functions*: The settings of the protection functions could be tampered. Protection elements could be exploited. Therefore the IEDs can be in mal-operation or being completely disabled. (iii) *Tripping/closing signals*: These signals are rather important as they have direct control over the circuit breaker. (iv) *Communication between relays*: These are usually digital status or control signals to perform inter-tripping or interlocking actions. (v) *Ethernet communication*: Whilst providing convenience for engineers to manage the IEDs, it potentially also gives hackers the possibility of remotely accessing the IEDs. When designing the test cases for IEDs, all these different areas should have a good coverage so that the IEDs are being tested thoroughly.

In the meantime, it is also very important to understand and identify the risk. The risk is a composite of probability and impact. Whenever a test case has been designed, its probability and impact should be analysed at the same time. In practice, given the same time scale and budget, it is worthwhile to focus on those that have both higher probability and impact.

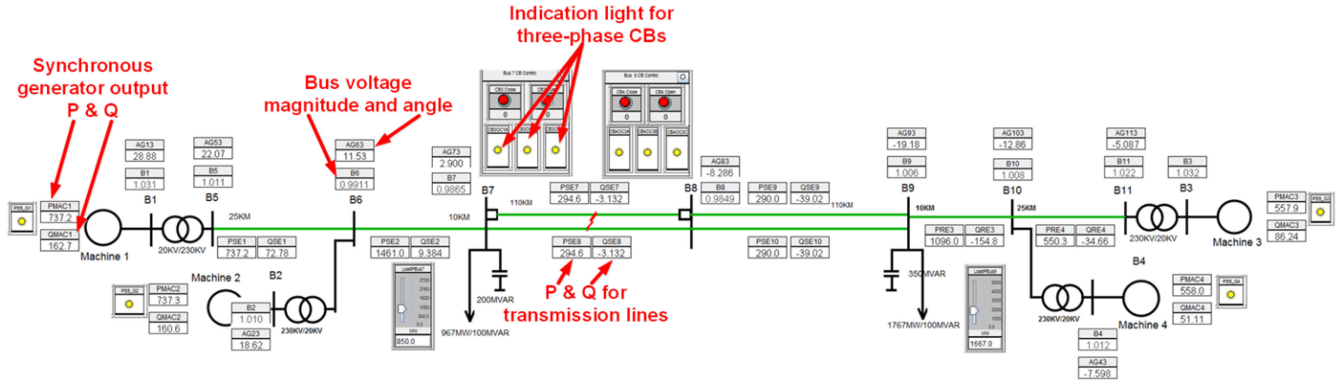

Fig. 4 *RTDS SCADA system*

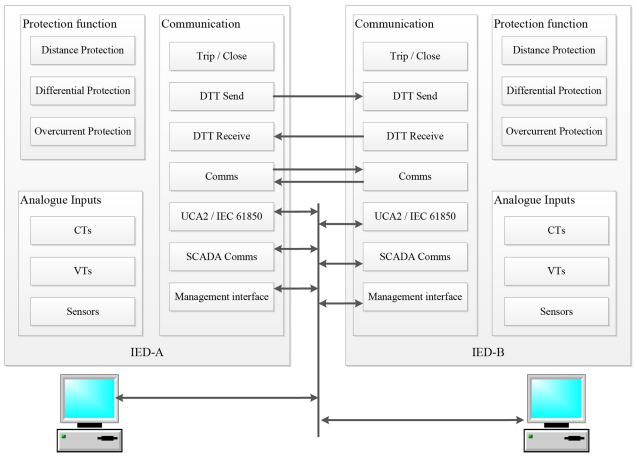

Fig. 5 *IEDs and their communication*

Last but not least, when a test case is being designed, it is also very important to consider what kind of test system it should use. For a test only focus on single equipment, a simple test system can be used. As an example, in this study, as shown previously in Fig. 1, Kundur's two-area four-machine system was used. On the other hand, when conducting test cases where the cascading effect is expected, a larger power system should be considered. For example, an IEEE 39-bus system was implemented in RTDS for conducting wider area system impact as shown in Fig. 6 [9]. Furthermore, it is also possible to replicate a practical power system within RTDS if required, as long as the system topology and parameters are available.

3 Case studies

Three test scenarios are presented in this section, to conduct cyber events and evaluate their impacts on the reliability, security, and safety of network operation for conventional P&C systems. The first case studies the system behaviour of a disabled tripping signal during faults. The second case focuses on the effects of tampered delayed auto reclosure. Both cases are based on the two-area four-machine system as shown in Fig. 7. The RTDS-based HIL testing platform is used to simulate these cases. The third case study investigates susceptibility to replay GOOSE message.

3.1 Case 1: disabled trip signal at one end

In this case study, a permanent three-phase to ground fault is applied at the middle (50% length) of the transmission line (TL78b) between Bus 7 and Bus 8. Two circuit breakers (CBs), CB1 and CB2, are located at each end of the transmission line. An attack of the disabled tripping signal of CB2 is simulated.

As shown in Fig. 8, the fault happens at 0.036 s, the trip signal from the relay is pulled high at 0.057 s. The control signal of the CB1 changes at 0.067 s and the CB1 is opened at 0.067 s. The trip signal of the CB2 stays at high as it is disabled. However, the CB2

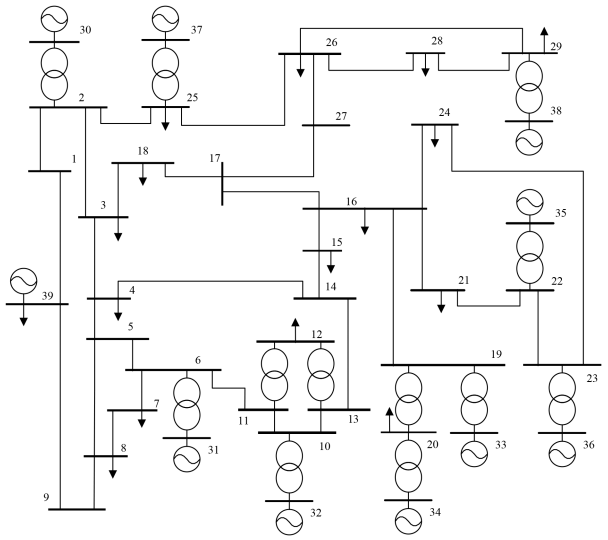

Fig. 6 *Schematic of an IEEE 39-bus system*

successfully opens at 0.087 s when receives the direct transfer trip (DTT) signal from the CB1.

In a case of the disabled trip signal at one end, tripping can only be achieved with the DTT signal from the other end. The attack may trigger malfunction of circuit breakers or disable the functionality of the circuit breaker. This could cause regional power loss or lead to wider area system blackout.

3.2 Case 2: tampered delayed auto reclosure

In this case study, fully customisable and configurable external delayed auto-reclose (DAR) has been modelled in RTDS. A temporary three-phase to the ground fault of 140 ms is applied on the transmission line TL78b between bus 7 and bus 8. The circuit breaker behaviour and power transmissions on TL78a and TL78b in both normal and tampered cases are compared to evaluate the impacts of this kind of attack.

In normal status, as shown in Fig. 9, the fault applies at 0.1248 s. The two circuit breakers, CB1 and CB2, open at 0.1544 s. DAR initiates at 1.1784 s. The DAR delay time is set to 1 s.

It can be seen from Fig. 10 that the currents, active and reactive power of TL78b increases as the fault applies and soon drops to 0 as both CBs opens. On the other hand, the currents and power of the parallel transmission line TL78a drop as the fault applied and increases significantly after both CBs open. Both lines are able to get back to the nominal working state after DAR.

If the healthy check signal of the CB2 is tampered or disabled, creating false healthy status, malfunction of DAR may be triggered or the functionality of DAR may be disabled. In this case, the DAR function is 'unhealthy' at CB2 and the reclosure will not be achieved at both ends. As shown in Fig. 11, the same temporary fault is applied and CB1 and CB2 are opened. However, the expected auto reclosure is not successful and both circuit breakers stay open.

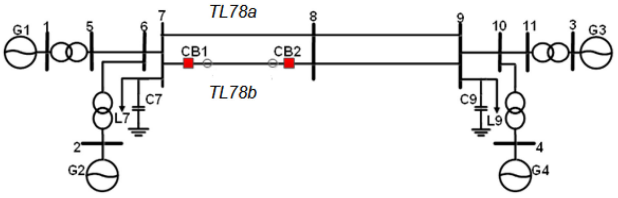

Fig. 7 *Kunder's two-area four-machine system*

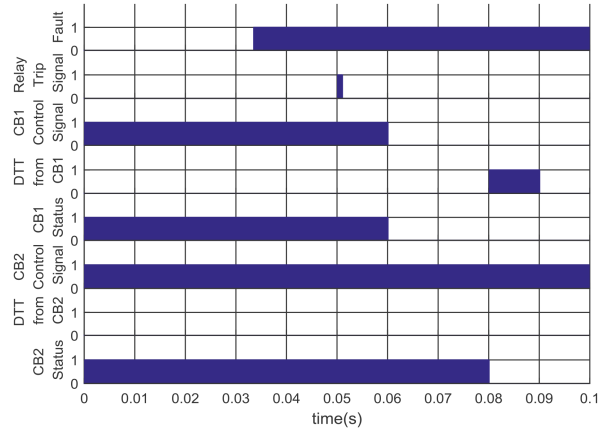

Fig. 8 *Disabled trip signal at one end*

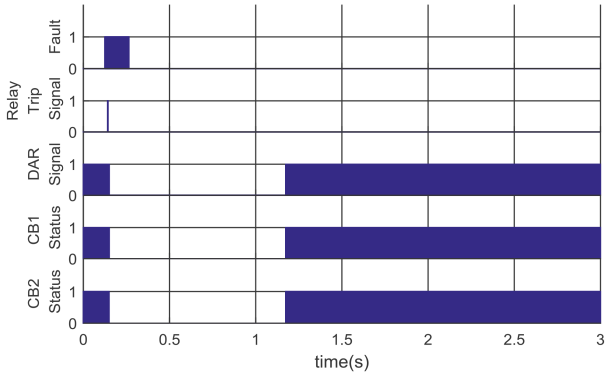

Fig. 9 *Normal case*

As shown in Fig. 12, the currents, the active and reactive power of TL78b drop and stay at 0 as both CBs open. The power supposed to be a transmission on TL78b is forced to TL78a, causing the currents, active and reactive power of TL78a increase significantly, which largely affects the system reliability. This kind of attack could cause regional power loss or lead to wider area system blackout.

3.3 Case 3: susceptibility to replay GOOSE messages

This test case aims to validate the susceptibility to replay GOOSE messages. In this test case, an IEC-61850 compatible feeder protection relay is used. It has been set to receive a binary signal sent from RTDS. The binary signal has then been bounced to VB001 as a virtual bit in the relay and tied to PB4A_LED, which is the upper LED of push button 4 on the front panel. In RTDS, a toggle controller has been used to control the corresponding binary signal. To test the susceptibility of GOOSE messages, two stages are designed. In stage one, set the toggle switch to OFF in RTDS simulation so that RTDS will keep sending the OFF message to the relay. Wireshark is used to capture the corresponding GOOSE message packet. The state of the packet is then altered to ON and the packet is then replayed back to the network.

The relay did not acknowledge the altered packet and the LED is still showing OFF state. This is possible due to the status number (StNum), sequence number (SqNum) and time value in the packet are not updated accordingly so that the relay refuse to change the status of the corresponding signal.

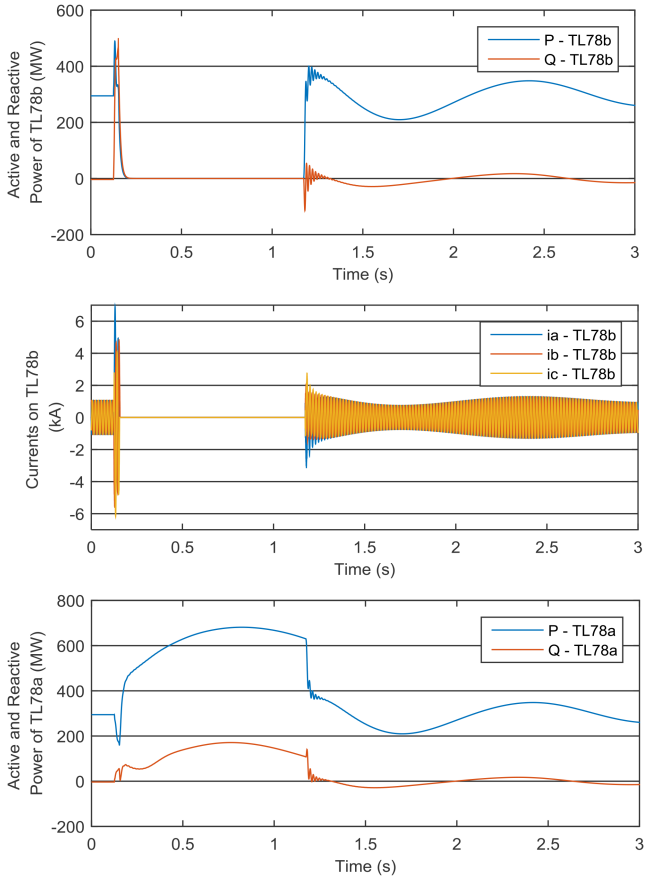

Fig. 10 *Current and power for the normal case*

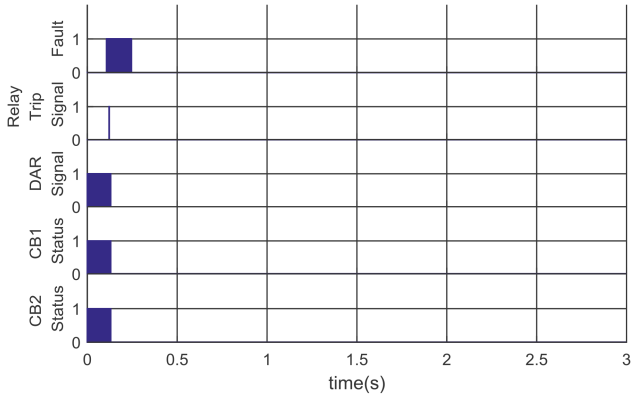

Fig. 11 *Disabled health signal for CB2*

In stage two, IED Explorer is used to reproducing GOOSE messages being sent from RTDS. IED Explorer is able to capture GOOSE messages in the network. The dataset captured can be automatically analysed and modify. Its GOOSE sender function, as shown in Fig. 13, can then import such a dataset and replay in the network. Such a function is considered as forging a genuine GOOSE message and is expected to be accepted by the subscribed IEDs.

Time, StNum and SqNum values are increased accordingly and synchronised while being transmitted. It appears that the relay acknowledges such messages and set corresponding front panel LED to ON state. However, it flips between ON and OFF due to receiving two different message streams. Potentially, there is a risk if the attacker managed to attach a device to craft certain packets, it can tamper or disable the corresponding IED input or output, which could result in wider area power system failure.

4 Conclusion

In this paper, an RTDS-based HIL testbed was designed, implemented and adapted as appropriate for the HIL testing of

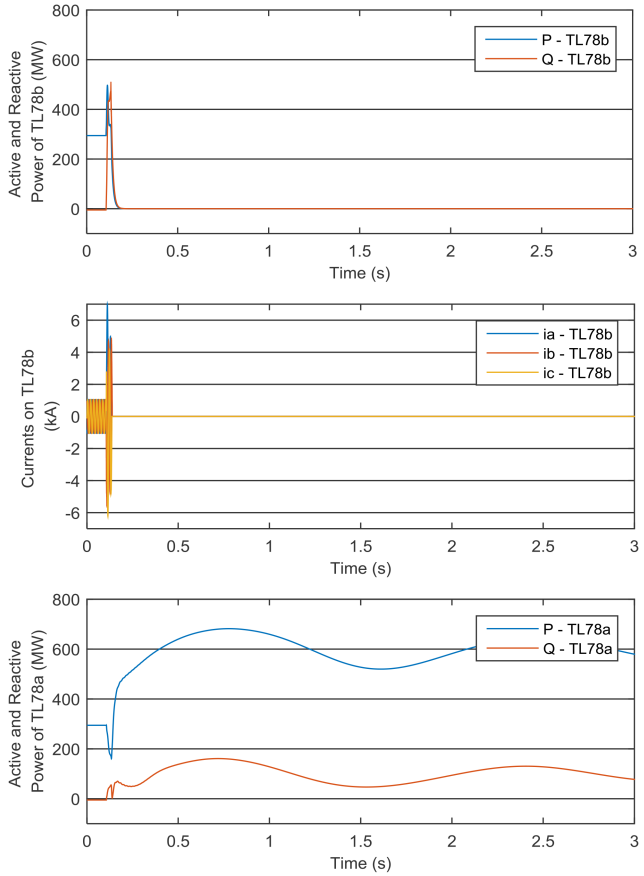

Fig. 12 *Current and power for the unhealthy case*

P&C equipment/functions of the pre-defined P&C systems. HIL tests through both standard electrical and emerging IEC- 61850-based interfaces have been presented. The basic concepts of designing test cases for IEDs have also been discussed. The performance of this testing platform has been tested and validated against tampered or disabled equipment. The developed HIL testing platform is an effective tool that can be used to conduct cyber physical studies by simulating different cyber-attacks and fault events to the power system. The standard power system bench mark system can be modelled in the HIL testing platform. Moreover, given realistic system and equipment parameters, the practical system can also be replicated within the HIL testing platform, which would be useful for investigating specific intentional attack for a regional or wider area network in real life. The HIL testing platform is scalable and can be repeatedly used for testing P&C system to ensure the stability, reliability and security of the future smart grid.

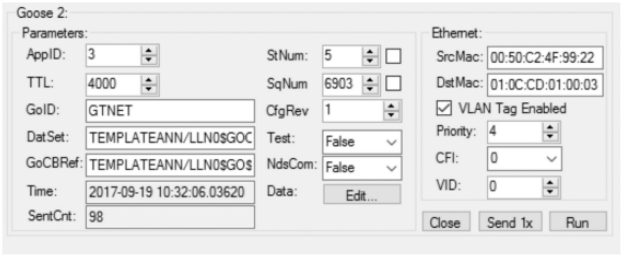

Fig. 13 *IED explorer GOOSE sender*

5 Acknowledgments

This work is from a Network Innovation Allowance Project in collaboration with National Grid, UK. This project was sponsored by the Office of Gas and Electricity Markets and the UK EPSRC under grant no. EP/M002845/1.

6 References

[1] Chakhchoukh, Y., Ishii, H.: 'Coordinated cyber-attacks on the measurement function in hybrid state estimation', *IEEE Trans. Power Syst.*, 2015, **30**, pp. 2487–2497

[2] Dae-Hyun, C., Le, X.: 'Ramp-induced data attacks on look-ahead dispatch in real-time power markets', *IEEE Trans. Smart Grid*, 2013, **4**, pp. 1235–1243

[3] Ye, H., Ge, Y., Liu, X., *et al.*: 'Transmission line rating attack in two-settlement electricity markets', *IEEE Trans. Smart Grid*, 2016, **7**, pp. 1346–1355

[4] Zhang, H., Cheng, P., Shi, L., *et al.*: 'Optimal denial-of-service attack scheduling with energy constraint', *IEEE Trans. Autom. Control*, 2015, **60**, pp. 3023–3028

[5] Chang, R.: 'Defending against flooding-based distributed denial-of-service attacks: a tutorial', *IEEE Commun. Mag.*, 2002, **40**, (10), pp 42–51

[6] Mo, R.C.Y., Sinopoli, B.: 'Detecting integrity attacks on SCADA systems', *IEEE Trans. Control Syst. Technol.*, 2014, **22**, pp. 1396–1407

[7] Zhang, F., Sun, Y., Cheng, L., *et al.*: 'Measurement and modeling of delays in wide- area closed-loop control systems', *IEEE Trans. Power Syst.*, 2015, **30**, pp. 2426–2433

[8] Tian, J., Liu, Z., Shu, J., *et al.*: 'Base on the ultra-short term power prediction and feed-forward control of energy management for microgrid system applied in industrial park', *IET Gener. Transm. Distrib.*, 2016, **10**, pp. 2259–2266

[9] Pai, A.: '*Energy function analysis for power system stability*' (Springer, New York, NY, USA, 1989)