Cyber-Resilience Lab

Demonstration Use-Case

Terms of Use

The current document describes a Use Case developed by *OFFIS e.V.* under the project Cyber-Resilience Lab, in cooperation with the Federal Ministry for Economic Affairs and Energy. The contents of this document provide an explanation to provide the reader with the instructions for proper interaction with the real time simulation environment run in this Use Case. Additionally, this document describes an on-line mock-up version of this use case which allows the reader to execute a simplified version of the use case, consisting in merely animations.

The pre-requirements for running the on-line mock-up demo is to install *Microsoft PowerPoint 2010* or newer versions. For running the real-time simulation environment and run the use case, please contact Dr. Davood Babazadeh (davood.babazadeh@offis.de) to set an appointment.

Why care about this?

The Cyber-Resilience Lab gives, in short, the possibility to analyze the integration of ICT and digital technologies in power systems through the use of its real-time components and software. In this sense, the vulnerabilities of the whole Cyber-Physical system is extended not only to overall physical malfunctions, but also to cybernetic phenomena. This use-case is conceived for educational purposes to show how such vulnerabilities, namely a cyber-attack, could unchain the disconnection of a small electrical distribution system. Furthermore, the use-case shows how a digital twin of the power grid may be used for detection and defense against these sort of attacks.

About the Use Case

The Graphical User Interface (GUI) of the Cyber-Resilience Demo is shown below:

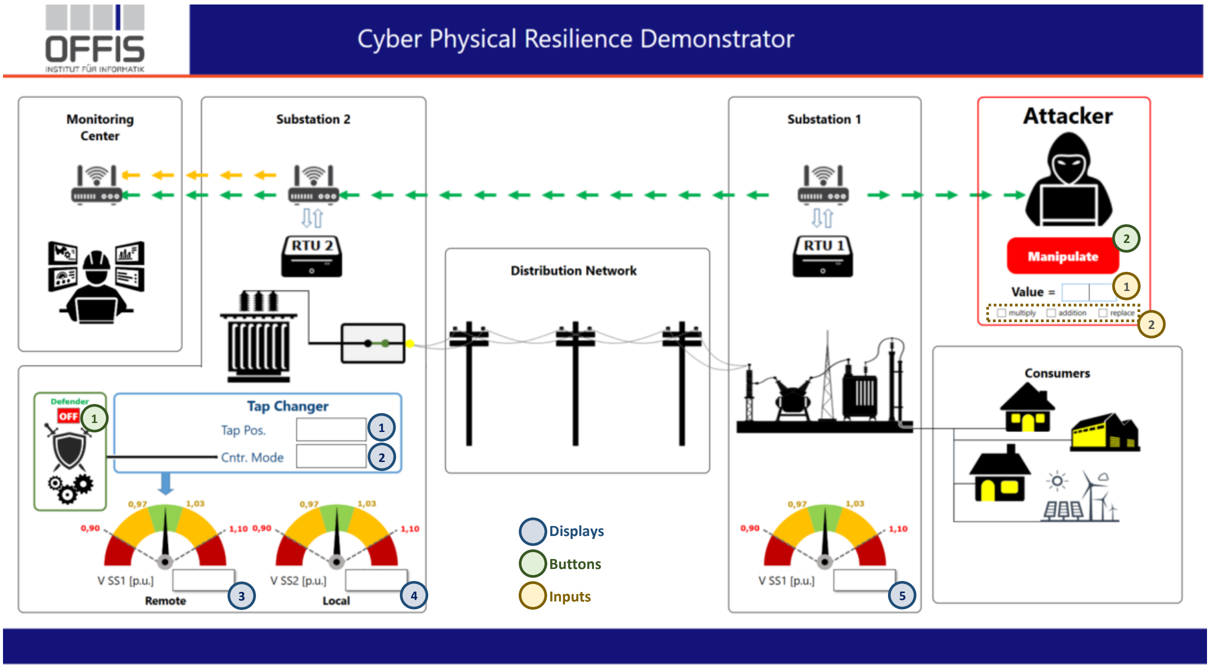


Figure 1 - Graphical User Interface of the Cyber-Resilience Demo

The topology for this use case consists on a simple Medium Voltage (MV) distribution radial feeder connecting two substations: *"Substation 1"* which provides electrical power to a residential load zone, and *"Substation 2"* which is connected to the electrical transmission system.

"Substation 2" counts with an On-Load-Tap-Changer (OLTC) transformer which is equipped with a voltage controller with two control modes: *"Remote"* and *"Local"*. The *"Remote"* mode is set under normal operation and controls the voltage of the remote *"Substation 1"*, whilst the *"Local"* mode controls the voltage of the local *"Substation 2"* under circumstances in which remote information cannot be trusted.

The objective of the controller is to keep the voltage at the controlled busbar within the values 0,97-1,03 per unit (p.u.) by adjusting the transformer's tap position. Specifically, the controller reduces the tap position in one step when it senses a voltage below 0,97 p.u. for longer than 10 seconds, and increases one step when it senses a voltage above 1,03 p.u. for longer than 10 seconds.

The information of both substations is digitally transmitted to the controller through Remote Terminal Units (RTU). Specifically, the information of *"Substation 1"* is transmitted to the controller in "Substation 2" via IEC 60870 5 104 protocol messages, and the information of *"Substation 2"* is transmitted locally via IEC 61850 protocol messages.

This use case exploits the vulnerabilities of the RTU located at *"Substation 1"*, in which a cyber-attacker retrieves the information sent to *"Substation 2"* and is able to alter its payload. By doing so, the attacker can alter the remote voltage value received by *"Substation 2"*, forcing tap adjustments in the transformer. These tap adjustments may eventually cause an under or overvoltage at the substations, triggering the respective protection, thus disconnecting the feeder from the electric mains. In this case, the switch located between the transformer and the feeder opens if the local *"Substation 2"* voltage is below 0,90 p.u. or above 1,10 p.u.

Additionally, the transformer's controller possesses a *"Defender"* who acts on its control mode: *"Remote"* and *"Local"*. The *"Defender"* consists on a Digital Twin (DT) of the feeder, which is provided with data acquired from the sensing devices in *"Substation 2"*, namely its voltage and the electrical current at the head of the feeder. The *"Defender"* compares the voltage value received from *"Substation 1"* with the voltage estimated by the DT. If these voltages do not match (providing a difference tolerance of 0,01 p.u.), the *"Defender"* changes the control mode of the controller to *"Local"*, given that the confidence on the remote voltage value is lost. Only when the threat has been detected and fixed, the *"Defender"* will detect matching voltages, and changes the default control mode *"Remote"*. In this use case, the defender may be either switched *"On"* and *"Off"*, allowing the user to compare its effect on the system in both situations.

Finally, the *"Monitoring Center"* receives the information from both substations via IEC 60870 5 104 messages. In this Demo, the *"Monitoring Center"* does not play a major role in the aim of the use case.

The description of the displays and the buttons of the GUI (*Figure 1*) of the Cyber-Resilience Demo is presented:

Displays

① Tap Position of the transformer.
② Control mode of the transformer's controller.
③ Voltage value of *"Substation 1"* received in *"Substation 2"*.
④ Voltage value of *"Substation 2"* measured locally.

⑤ Voltage value of *"Substation 1"* measured locally.

Buttons

① Switch *On Off* of the *"Defender"*.

② Cyber-attack button – when pressed, the voltage value sent to "Substation 2" will be modified according to inputs ① and ②.

Inputs

① Value by which the action checked in ② will be applied to the local voltage value in *"Substation 1"*, this is to say ⑤.

② Check box (only one may be selected) – specifies the action to alter value ⑤. It either multiplies it by ①, adds it to ① or replaces it for ①.

Tools used in the Use Case

The Cyber-Resilience Demonstration Use Case consists on a real-time simulation environment, making use of the following software:

ePHASORSIM *OPAL-RT*	Modelling of the feeder (Load, line, busbars and transformer)
eMEGASIM *OPAL-RT*	Modelling of the tap changer controller of the transformer and the DT of the system
EXata *SCALABLE Network Technologies*	Modelling of the communication infrastructure between the substations in IEC 60870 5 104
Virtual RTU *OFFIS*	Communication protocol translation and modelling of payload alteration options (Cyber-attacker modelling)

About on-line mock-up version of the Use Case

A simplified mock-up version of the Use Case is available to provide the user an example on how the original Use Case works. This mock-up version consists in animations developed using *Microsoft PowerPoint 2010*.

When accessing the file, the selection menu shown in Figure 2 will appear on screen. Two buttons are available in this window

- Successful Cyber-Attack: This selection Button will show a different window in which the Use Case topology is shown and the Defender is out of service (*Off*). In this option, a cyber-attack is executed by pressing the button "Modify Value", shown in Figure 3. The cyber-attack consists in the multiplication of the value acquired from *"Substation 1"* by 0,9, thus sending the transformer's controller a low voltage. The transformer reacts by changing its tap position to bring this altered voltage back to its permissible range. However, this causes an overvoltage at the substations, leading to the disconnection of the feeder triggered by the overvoltage protection in "Substation 2". Once the feeder is disconnected the animation is completed. It is possible to go back to the *Selection Window* by pressing the button "Back to Menu" (Figure 3).

- Cyber-Attack countered by Grid Defender: This selection Button will show a different window in which the Use Case topology is shown and the Defender on service (*On*). In this option, a cyber-attack is executed by pressing the button "Modify Value", shown in Figure 3. The cyber-attack consists in the multiplication of the value acquired from *"Substation 1"* by 0,9, thus sending the transformer's controller a low voltage. The transformer reacts by changing its tap position to bring this altered voltage back to its permissible range. In this case, the Digital Twin equipped in the Defender detects that the received voltage is different from the expected voltage, based on the local measurements it acquires. Therefore, the defender changes the control mode of the controller to "Local", preventing undesired tap changes.

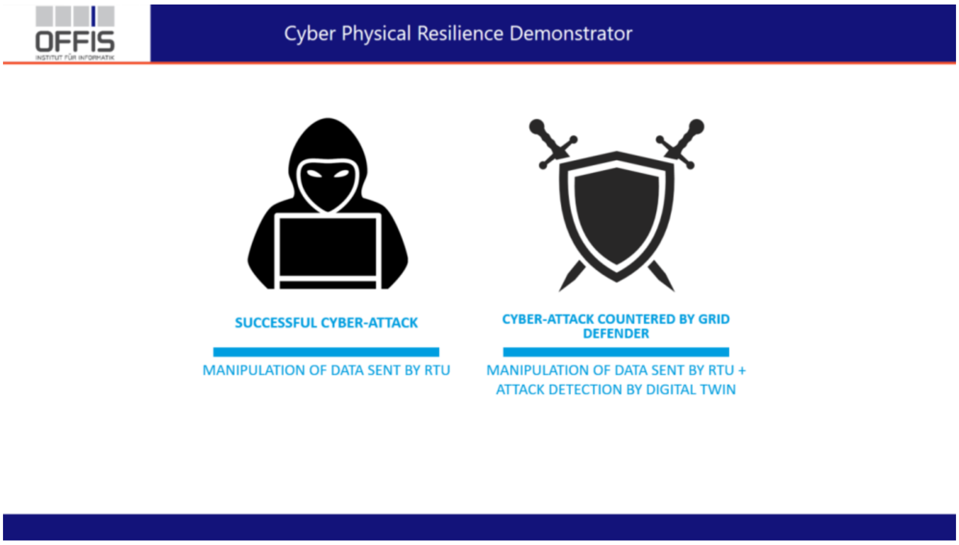
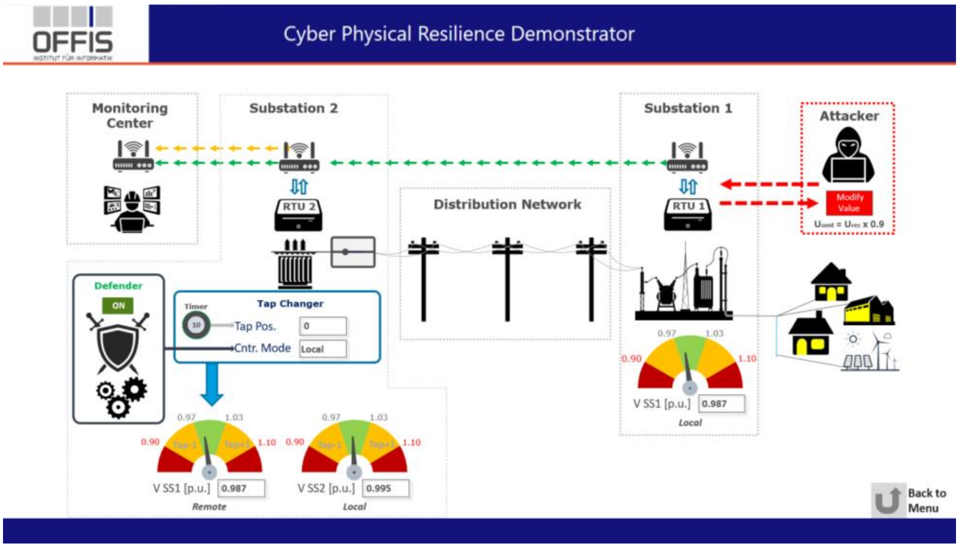

OFFIS
INSTITUT FÜR INFORMATIK
Cyber Physical Resilience Demonstrator
SUCCESSFUL CYBER-ATTACK
MANIPULATION OF DATA SENT BY RTU
CYBER-ATTACK COUNTERED BY GRID DEFENDER
MANIPULATION OF DATA SENT BY RTU + ATTACK DETECTION BY DIGITAL TWIN

Figure 2 - Selection Menu of the Use Case Mock-Up version



Tap Pos. 0

Cntr. Mode Local

V SS1 [p.u.] 0.987

Remote

V SS2 [p.u.] 0.995

Local

V SS1 [p.u.] 0.987

Local

Figure 3 - GUI of the Use Case Mock-Up version - Defender ON Selection