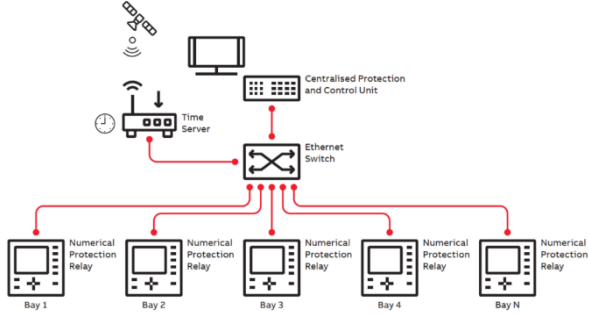


Test Case 22

Authors Vetrivel S.R., A. Stefanov, and S. Vogel
 Project ERIGrid 2.0

Version 3
 Date 28/04/21

Name of the Test Case	Resilience Assessment of ICT infrastructure
Narrative	The broad aim of this test case is to quantify and assess the resilience of ICT equipment used for communication in Cyber Physical Systems (CPS), i.e., smart grids. More specifically, the focus is on cyber resilience of digital substations . In a digital substation, analogue signal wiring is replaced with digital Ethernet (IEEE 802.3) links. Communication within a digital substation is realized through the IEC 61850 standard that covers substation automation and protection functionalities. Communication with the control center is realized through a dedicated communication gateway using protocols such as IEC 60870-5-104 and/or DNP 3. CPS resilience assessment considers the impact on power grid operation, when the abovementioned protocols/standards in digital substations are subjected to disturbances or targeted cyber attacks – packet loss, denial of service, etc. The characterization of this performance is one of the major interests of this test case, considering the nature of communication effects, and their overall impact on grid operations.
Function(s) under Investigation (FuI) “the referenced specification of a function realized (operationalized) by the object under investigation”	<ul style="list-style-type: none"> • Protection and automation functionality in a digital substation. • Type of data exchanged, i.e., control commands and measurements.
Object under Investigation (Oul) “the component(s) (1..n) that are to be qualified by the test”	Digital substation (see SuT for more information)
Domain under Investigation (Dul): “the relevant domains or sub-domains of test parameters and connectivity.”	<ul style="list-style-type: none"> • Information and Communication Technology (ICT) • Electrical
Purpose of Investigation (Pol) The test purpose in terms of Characterization, Verification, or Validation	<p>Verification and characterization of cyber resilience of digital substations. Specifically, characterize and verify the impact of ICT infrastructure performance on grid operations, in a digital substation in the presence of:</p> <ol style="list-style-type: none"> 1. Component failures in the ICT infrastructure of the substation 2. Misconfiguration of the ICT infrastructure 3. Cyber attacks targeting the substation ICT infrastructure <p>The impact on grid operations is measured by noting how aforementioned factors affect protection functionality, i.e., tripping times in a digital substation.</p>

<p>System under Test (SuT): Systems, subsystems, components included in the test case or test setup.</p>	<p>A digital substation includes substation bays, merging units, Ethernet switches (representing the process bus), Human Machine Interfaces (HMIs), time servers, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), centralized protection and control units, station control systems, etc. A substation bay comprises busbars, disconnectors, circuit breakers, current and voltage transformers (CTs and VTs), etc. Hence, to realize this test case, the following components are required:</p> <ul style="list-style-type: none"> Real-time grid simulator such as RTDS or OPAL-RT that supports Hardware-in-Loop (HIL) studies Substation network elements: <ol style="list-style-type: none"> At least one ethernet switch and time server. At least two or more physical IEC 61850 capable IEDs RTUs, MUs, other HIL devices A communication network emulator/simulator to model disturbances/cyber attacks <p>The testing involves interfacing the real-time grid simulator with all hardware components in a HIL setup to mimic a digital substation. Furthermore, the real-time grid simulator also needs to be interfaced with the network emulator to model and input communication related effects such as latency, packet loss, loss of service, etc.</p>  <p>Source: Centralized Protection and Control. ABB Whitepaper. 2020.</p>
<p>Functions under Test (FuT) Functions relevant to the operation of the system under test, including Ful and relevant interactions btw. Oul and SuT.</p>	<ul style="list-style-type: none"> Capability of the real-time grid simulator to exchange data using IEC 61850 and IEC 60870-5-104 Automation and protection functionality realized by Oul Behaviour and performance of IEDs within the SuT, when subjected to specific disturbances Emulation of communication networks Performance of communication network emulator, i.e., Mininet
<p>Test criteria (TCR) Formulation of criteria for each PoI based on properties of SuT; encompasses properties of test signals and output measures.</p>	<ul style="list-style-type: none"> Equipment response and performance under normal operating conditions Equipment response and performance when subjected to communication-based disturbances – packet losses, latency, etc.

	<ul style="list-style-type: none"> System response to communication-based disturbances
Target Metrics (TM) Measures required to quantify each identified test criteria	<ol style="list-style-type: none"> Tripping times <ul style="list-style-type: none"> During normal operating conditions During disturbances Communication of control commands (GOOSE) <ul style="list-style-type: none"> During faulted (short-circuit) conditions During communication disturbances
Variability Attributes (VA) controllable or uncontrollable factors and the required variability; ref. to Pol.	<ul style="list-style-type: none"> Type of protection scheme implemented Overall substation configuration and topology Characteristics of network emulator Redundancy (N-1, N-2.... N-k): Number of components or communication links which can fail before system operation is at risk Topology and type of simulated power system (transmission vs distribution) Type of cyber-attack, e.g., Denial-of-Service (DoS), malformed authentication codes, etc.
Quality Attributes (QA) threshold levels for test result quality as well as pass/fail criteria.	<ul style="list-style-type: none"> Real-time communication performance during normal, electrical fault and communication disturbance conditions Pass: performance within max threshold of 10 ms Fail: performance exceeds 10 ms under any conditions

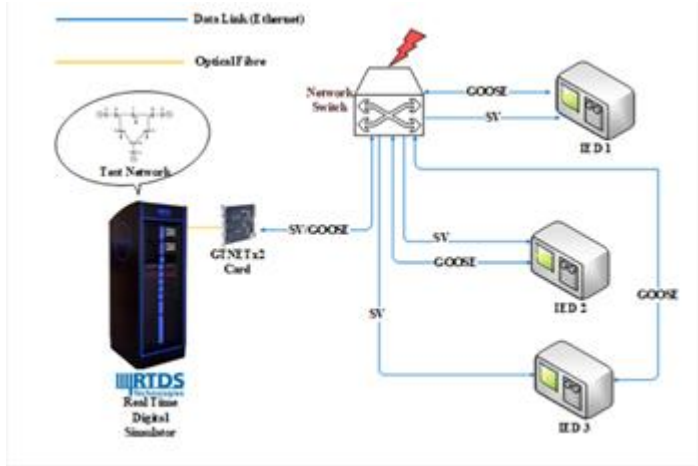
Qualification Strategy

The Pol are mainly addressed by characterizing and verifying the impact of ICT infrastructure performance on grid operations, in a digital substation. This can be achieved by determining how protection functionality and thereby power system stability is affected by disturbances to ICT infrastructure.

- As per the IEC 61850 standard, the maximum tripping time for protection equipment should always be lesser than 10ms. Hence, this can be used as a metric to assess the cyber resilience of a digital substation. This assessment is subject to presence of component failures in the ICT infrastructure of the substation, misconfigurations, and cyber attacks targeting the substation ICT infrastructure.

Test Specification TC22.TS1

Reference to Test Case	TC22
Title of Test	Determination of maximum tripping times in the presence of ICT disturbances within a digital substation
Test Rationale	The IEC 61850 standard recommends a maximum time for transmission of fast messages such as trip signals to be within 10ms. Hence, this experiment seeks to test this performance requirement under adverse communication related conditions such as packet losses, latency, etc.
Specific Test System	The test system comprises of a real-time grid simulator, at least

(graphical)	<p>one Ethernet switch, and multiple IEC 61850 devices interconnected in a HIL setup. See SuT for further information.</p> 
Target measures	The maximum time taken to communicate trip signals when subjected to specific communication disturbances.
Input and output parameters	<p>Input parameters:</p> <ul style="list-style-type: none"> Type of power system simulated Network topology of substation Protection schemes applied through the relays Fault type and duration Type of disturbance: equipment failure, increased latency, bad actor, misconfiguration etc. <p>Output parameters:</p> <ul style="list-style-type: none"> Maximum time taken to communicate trip signals
Test Design	<p>The test is a HIL experiment as described in the SuT and specific test system. The test design is as follows:</p> <ol style="list-style-type: none"> 1. Start the system with all devices functioning as required. 2. Run a test simulation with a short-circuit condition 3. Note that appropriate relay communicates trip signal via IEC 61850 GOOSE message 4. Circuit breaker is opened, and the fault is cleared 5. Note this tripping time as T1 6. Apply a specific type of communication disturbance, for e.g., increased network traffic via an external device or network emulator. 7. Repeat steps 2 to 4 and note the new tripping time T2. 8. Repeat steps 6 and 7 in case of equipment failures, mis-configurations, and note times as T3, T4, and so on.
Initial system state	<ul style="list-style-type: none"> All devices are ON and running Real-time grid simulator can send and receive messages to and from the hardware devices
Evolution of system state and test signals	Successful recording of parameters T1, T2...Tn for various types of ICT disturbances
Other parameters	N/A
Temporal resolution	Tens of milliseconds
Source of uncertainty	Configuration of ethernet switch, IEC 61850 device compatibility
Suspension criteria / Stopping criteria	<p>Suspension criteria: Errors in devices/misconfiguration</p> <p>Stopping criteria: the experiment can be concluded when the maximum tripping times for various combinations of ICT disturbances and fault types are noted. Alternatively, if this time ever exceeds 10ms, the experiment can be stopped.</p>